NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

EFFECTIVENESS OF USING RED TEAMS TO IDENTIFY MARITIME SECURITY VULNERABILITIES TO TERRORIST ATTACK

by

Anna M. Culpepper

September 2004

Thesis Advisor:	Raymond Buettner, Jr.
Thesis Co-Advisor:	Dorothy Denning

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE		Form Approved OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	September 2004	Master's Thesis

4. TITLE AND SUBTITLE: Effectiveness of Using Red-Teams to Identify Maritime Security Vulnerabilities to Terrorist Attack	5. FUNDING NUMBERS
6. AUTHOR Anna M. Culpepper	
7. PERFORMING ORGANIZATION NAME AND ADDRESS Naval Postgraduate School Monterey, CA 93943-5000	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING /MONITORING AGENCY NAME AND ADDRESS N/A	10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT	12b. DISTRIBUTION CODE
Approved for public release; distribution is unlimited	A

13. ABSTRACT (maximum 200 words)

As the United States continues to develop plans and policies to counter the threat of terrorism, it becomes increasingly more vital to understand the entire spectrum of the threat. Realistically assessing the capability of possible and probable terrorist groups helps federal and state agencies to establish potential methods and procedures for defense and maritime domain awareness. Yet, the avenues of attack and the varieties of terrorists far outnumber the available resources of most agencies concerned. Moreover, there have been no attacks on homeland U.S. targets since September 11. The red team concept provides an innovative method to examine these vulnerabilities from the terrorist perspective. The effectiveness of a red team can be measured in various ways and is dependent on key organizational and situational elements. In the end, the determination of effectiveness is based on the original intentions of the host enterprise, whether it is training, research, strategy, or analysis or a combination. We conducted a case study to utilize the red team concept as a tool for bringing a fresh awareness to a critical issue within the National Strategy for Combating Terrorism. The red teams identified vulnerabilities of possible targets, raised the awareness on the nature of terrorists, researched potential tactics and tools, and examined existing assumptions about maritime security. In applying the red team concept, the case study used military officers as surrogate terrorists planning a campaign to attack port cities. The case study effectively demonstrated the anticipated functions, while the follow-on actions ensured that the results were distributed to the appropriate agencies. Furthermore, civilian officials and the agencies concerned valued the red team reports as positive insights into the current situation.

14. SUBJECT TERMS Information Operations, Red Team, Operations Research, Terrorism, Defense Analysis	15. NUMBER OF PAGES 87
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	UL

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

EFFECTIVENESS OF USING RED-TEAMS TO IDENTIFY MARITIME SECURITY VULNERABILITIES TO TERRORIST ATTACK

Anna M. Culpepper
Lieutenant, United States Navy
B.A., William Marsh Rice University, 1997

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN SYSTEMS ENGINEERING

from the

NAVAL POSTGRADUATE SCHOOL
September 2004

Author: Anna M. Culpepper

Approved by: Raymond Buettner, Jr.
Thesis Advisor

Dorothy Denning
Thesis Co-Advisor

Dan Boger
Chairman, Department of Information Sciences

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

As the United States continues to develop plans and policies to counter the threat of terrorism, it becomes increasingly more vital to understand the entire spectrum of the threat. Realistically assessing the capability of possible and probable terrorist groups helps federal and state agencies to establish potential methods and procedures for defense and maritime domain awareness. Yet, the avenues of attack and the varieties of terrorists far outnumber the available resources of most agencies concerned. Moreover, there have been no attacks on homeland U.S. targets since September 11. The red team concept provides an innovative method to examine these vulnerabilities from the terrorist perspective. The effectiveness of a red team can be measured in various ways and is dependent on key organizational and situational elements. In the end, the determination of effectiveness is based on the original intentions of the host enterprise, whether it is training, research, strategy, or analysis or a combination. We conducted a case study to utilize the red team concept as a tool for bringing a fresh awareness to a critical issue within the National Strategy for Combating Terrorism. The red teams identified vulnerabilities of possible targets, raised the awareness on the nature of terrorists, researched potential tactics and tools, and examined existing assumptions about maritime security. In applying the red team concept, the case study used military officers as surrogate terrorists planning a campaign to attack port cities. The case study effectively demonstrated the anticipated functions, while the follow-on actions ensured that the results were distributed to the appropriate agencies. Furthermore, civilian officials and the agencies concerned valued the red team reports as positive insights into the current situation.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ABBREVIATIONS AND ACRONYMS

AIS	Automatic Identification System
APHIS	Animal and Plant Health Inspection Service
CAST	Center for Adaptive Strategies and Threats
CBP	Customs and Border Protection Bureau
CHOP	Countermeasures Hands-On Program
CJCS	Chairman, Joint Chiefs of Staff
CSI	Container Security Initiative
C-TPAT	Customs -Trade Partnership Against Terrorism
DART	Defense Adaptive Red Team
DHS	Department of Homeland Security
DOD	Department of Defense
DOS	Department of State
DSB	Defense Science Board
DTRA	Defense Threat Reduction Agency
FBI	Federal Bureau of Investigation
GAO	General Accounting Office
H&AI	Hicks & Associates, Inc.
INS	Immigration and Naturalization Service
JCS	Joint Chiefs of Staff
MDA	Missile Defense Agency
MEIC	Middle East Information Center
MTSA	Maritime Transportation Security Act of 2002
PLO	Palestinian Liberation Organization
SAFE	Strategy and Force Evaluation
SAGA	Strategy, Analysis & Gaming Agency
SSBN	Ballistic Missile Submarine – Nuclear
SSN	Submarine – Nuclear
TSA	Transportation Security Administration
TWIC	Transportation Worker Identification Card

VTS	Vessel Traffic Service
U.S.	United States (of America)
USBP	U.S. Border Patrol
USCS	U.S. Customs Service
USDA	U.S. Department of Agriculture

I. INTRODUCTION

A. BACKGROUND

How do we conduct a war versus a strategy as nebulous as terrorism? This question plagues the leaders of the United States, and since September 11, 2001, every city and government agency across the country. (Feith, 2004) From city officials to the President of the United States (U.S.), not only the responsibility to respond to a terrorist attack, but also the responsibility to prevent any future attacks has spread to every person concerned. Additionally, that fateful day proves that as a force, as a nation, the United States continuously needs to expand her repertoire in the art of war. The U.S. needs to employ the full spectrum of warfare in order to counter the threat of terrorism. At times, this will require preemptive action, and at others, it will require careful diplomacy, but in order to make these options and others more effective, it is necessary to understand the adversary we face. The necessity to dissect the decision-making process of an adversary is not new, but the adversary we face certainly is new to many. In so many ways, the methods of terrorist organizations are vague and hazy to the Western method of rational thinking. Some experts doubt that the ability exists in Western capitalists and Islamic fundamentalists to understand each other.

> Security and risk assessment professionals must always adapt proactive measures to anticipate, defend against, and preempt new types of terrorist attacks. Moreover, one should not expect past trends to necessarily reveal future attack patterns because terrorists, especially al-Qaeda planners always seek to exploit new vulnerabilities and new and innovative modes of warfare in order to evade detection and inflict maximum damage. (Sinai, 2003)

As researchers and military members, we have a responsibility to assist the efforts of these leaders and units as they engage this particular new type of adversary.

B. OBJECTIVE

> Practitioners of strategy and force planning constantly struggle to achieve a balance among many competing variables. The art of strategy and force planning is made evident by how well the inevitable tensions among these variables are resolved. (Bartlett, Holman, & Somes, 2000)

Using the Bartlett Model seen in Figure 1, the continuous and iterative nature of strategy and force planning is apparent. Divergent views of the current threats and vulnerabilities shape the debates on the national goals, strategies and means. Consequently, the assessment of the security environment requires strategists to examine the adversary and his strategic development. In this case, do terrorist organizations function similarly to states or businesses? Do they balance their goals and objectives with the risks and resources? Is it possible to influence or predict this process with our actions and reactions? Furthermore, are our forces prepared and capable to counter the threat of this new adversary? With resource constraints constantly limiting involvement, each choice represents a risk. In order to mitigate the level of risk in these choices, it is necessary to maintain the iterative nature, reassessing the security environment in light of the national goals and capabilities.

The objective of this thesis is to evaluate one method of risk mitigation, the red team concept, and its effectiveness in revealing and examining the inherent assumptions of the enterprise that employs it. By applying the red team concept to domestic port security, the case study aims to identify the maritime vulnerabilities to terrorist attack at three large Western cities. In addition, the red teams will evaluate the tools and tactics employed by terrorists to avoid detection while planning a terrorist attack. However, in any evaluation on the effectiveness of the concept, we must also consider the utility of the knowledge and the actions taken based on that knowledge. Therefore, this thesis will explore the red team concept and its applicability to counterterrorism and maritime security.

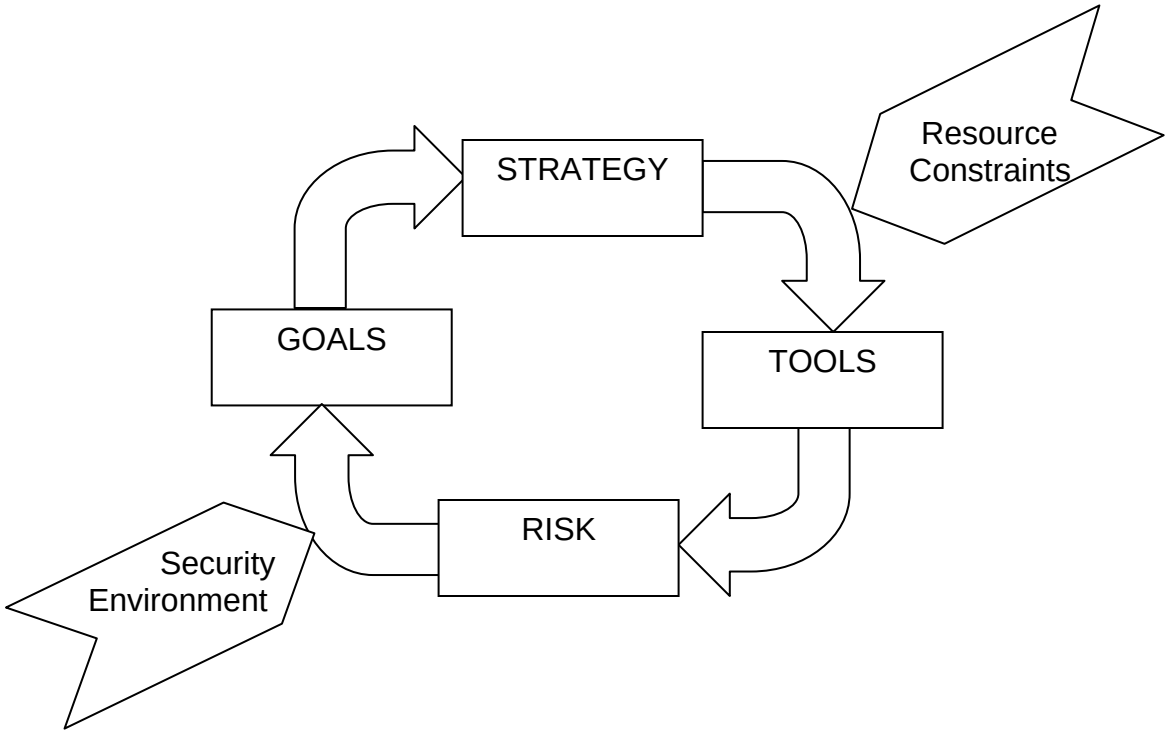

Figure 1: Bartlett Model of Strategic Development (Bartlett et al, 2000)

C. RELATED WORK

Other research relevant to this thesis involves two specific topics: counter-terrorism and the red team concept. There are countless experiments, debates, and projects pursuing the topic of terrorism and its subordinate fields. In addition, there are many experiments and research on the effectiveness of models, simulations and games. However, there are few efforts to research the effectiveness of models, simulations, and games in counter-terrorism. Yet, more enterprises are utilizing field exercises and war games to test their security measures and emergency responders in a terrorist attack. Consequently, research is necessary to examine the success of these exercises and improve their efforts.

> We believe red teaming is especially important now. Adversaries are tough targets for intelligence. Red teaming can both complement and inform intelligence collection and analysis. Aggressive red teams challenge emerging operational concepts in

> order to discover weaknesses before real adversaries do. Red teaming also tempers the complacency that often follows success. (DSB, 2003)

With these words, the Defense Science Board (DSB) tasked the Defense Adaptive Red Team (DART) to examine the red team concept in depth. Hicks & Associates, Inc., is the prime contractor for the DART and relies on "an extensive network of experts in terrorism, weapons of mass destruction, technology exploitation, cultural intelligence, media influence operations, information and communication systems attack, urban operations and war-gaming" in order to establish and disseminate best practices for conducting red-teaming throughout government agencies. (H&AI, 2004) However, at the beginning of this case study, DART had not yet published the findings from the Center for Adaptive Strategies and Threats (CAST) at H&AI. As of the conclusion of this thesis, only working papers were available. These papers discussed the future of Al Qa'ida, the historical use of red teams in the military and initial recommendations for red team usage.

Other organizations are using the red team concept specifically to counter terrorist efforts. Sandia National Laboratories is currently using red teams to identify potential terrorist attack methods and profiles in order to provide indicators and increase the quality of warnings from intelligence centers. However, the majority of their efforts focus on cyber warfare aspects rather than direct action or psychological operations. Joshua Sinai in coordination with the Red Team Journal has written articles discussing the uses of the red team to examine national strategies and assess emerging threats in the security environment. Additionally, cities such as Seattle and Salt Lake City, conduct annual exercises that include red teams to examine their security and emergency response systems. However, none of these efforts directly examines the effectiveness of using red teams to identify potential vulnerabilities to terrorist attack.

Therefore, in this case study, we attempt to utilize the red team concept in order to address this deficit, and if possible, to identify the critical elements and

the measures of effectiveness of the red team concept to ensure future successful applications. By building on the recommendation from DSB, we hope to complement the efforts of Sandia and the regional homeland security experts to counter and prevent terrorist attack.

THIS PAGE INTENTIONALLY LEFT BLANK

II. RED TEAM CONCEPT

A. HISTORY AND DEFINITIONS

One of the principles of war as stated by Sun Tzu is “determine the enemy’s plans and you will know which strategy will be successful and which will not.”(Sun Tzu, 1963) The attempt to determine the intentions of an adversary is an age-old idea. By considering how the enemy plans to attack, one can learn the best way to counter the attack and increase the likelihood of success. The United States has been using simulations, games and models since its inception, and especially in the last century, to address potential threats and strategies. Specifically, the United States Navy “established a strong gaming tradition between the world wars and carried these traditions forward into the age of high-tech gaming after World War II.” (Perla, 1990) After World War II, the United States routinely used games and simulations to address broad national security issues. (Hanley, 1991) Mostly due to the expense, the use of models, simulations, and games is preferred to field exercises in order to train leaders and research operational methods. (Brewer & Shubik, 1979) This led to machine-directed games to test and develop tactics and strategies. Furthermore, there are massive multi-player gaming capabilities throughout the Department of Defense (DOD) that require multiple processors with the highest processing speeds and the largest databases. Yet, verbal scenarios and seminar games, also known as free-form games, are more popular to address the broader strategic and allocation issues.

> The political and military free-form [model, simulation, & game] was designed primarily as a method of investigating substantive questions in political science rather than as a gaming methodology. Such games are usually played with a red team, a blue team, and control team. (Brewer & Shubik, 1979)

Even though our version of the red team for this case study is vastly different, the history of these attempts in war games and exercises has shaped our current red team concept and principles.

Although many may know what we mean by the term 'red team,' the definition we use in this thesis comes from the DSB Task Force on DOD Red Teaming Activities: "We define red teams broadly, including, not only playing the adversary, but also playing devil's advocate and related roles."(DSB, 2003) The purpose of the red team is to reduce risks and increase opportunities by challenging aspects of plans, programs, and assumptions. The shapes and sizes of red teams in past and current organizations vary widely. DSB further breaks the definition down into three specific types: surrogate adversaries and competitors, devil's advocates, and independent sources of judgment. Furthermore, when acting as surrogate adversaries, the red team tries to emulate the enemy, using his presumed tactics and weapons. (DSB, 2003) In this study, the red teams act as surrogate adversaries outside the usual exercise construct. In particular, due to the objectives of counterterrorism and homeland security, there is no specific blue team interacting with the red team – instead the red teams challenge the real agencies and personnel of the targets. The discussion of the case study will explain the structure in more detail (Chapter 6).

B. PAST AND CURRENT RED-TEAMING ACTIVITIES

In the United States, the history of war games, and, by extension – their red teams, is the most developed within the DOD. One of the best-remembered war games is the Strategy and Force Evaluation (SAFE) hosted by the Rand Corporation in the 1960s. It was an extremely well documented formal seminar with two teams consisting of highly trained and experienced strategic analysts. Rand provided both teams with a budget, a policy statement to guide decisions, a selection of available strategic forces, the current force postures of the United States and the Soviet Union, and the task of designing the future shape of the armed forces. The most important results of the SAFE games were the branch points (discarded courses of action) that inspired focused seminars to examine the consequences of strategy selection or rejection. (Brewer & Shubik, 1979) The Studies, Analysis, and Gaming Agency (SAGA) of the Pentagon was vital because "the hypothetical crises [were] treated intensively, and the game

environment serve[d] the important additional purposes of stimulating communication among agencies and assessment of personnel in a real-world environment." (Brewer & Shubik, 1979) One of the most celebrated and continual use of red teams is by the Nuclear Regulatory Commission, especially because, from 1991-2001, 37 of the 81 exercises conducted resulted in successful attacks against the targeted plant. In those exercises, the Commission created a permanent staff of red team members to act as surrogate adversaries and probe for security discrepancies. (Eckert, 2004)

Current red-teaming activities within the DOD vary in their objectives, their structures, and their perspectives. The U.S. Navy SSBN Security Program, acting as devil's advocates, assesses threats and vulnerabilities based on technological feasibility and operational realities. Their focus has shifted over the years to include force protection measures, terrorist threats, and in-port security, but the scope of their assessments is the same. The Missile Defense Agency (MDA) attempts to identify, characterize, understand and mitigate the risks associated with the development and deployment of systems through a threat-based technological approach. Their Countermeasures Hands-On Program (CHOP) examines unsophisticated threats to these systems. The Air Force Red Team designs and performs field tests to assess technological concepts. The Army Red Franchise, similarly to the SAFE games of the 1960s, is responsible for defining the operational environment for the next two decades, in order to shape the force and capability structure of the Army. The Joint Forces Command Red Teams participate in joint exercises and experiments that usually preclude or constrain free-play in the scenario. The Chairman, Joint Chiefs of Staff, designated the Defense Threat Reduction Agency (DTRA) to assist in his force protection responsibilities by performing vulnerability assessments at DOD installations worldwide. (GAO, 2002) Finally, the Office of the Secretary of Defense tasked the DART with providing red-team concept development and an evaluation framework while providing the full spectrum of red teams to DOD units. (DSB, 2003)

Non-governmental agencies are also applying operational gaming to address city and regional planning, transportation and ecological studies, economic forecasting, and, especially, emergency preparedness. (Brewer & Shubik, 1979) For example, Sandia National Laboratories is using red-teams to generate "specific hypothetical scenarios that can then be distilled into their component parts to deliver the desired operational methods." Their new "Hypothesizer" would serve as a database of possible terrorist tactics and scenarios as developed by the red teams, allowing analysts to assess the likelihood of potential attacks depending on the intelligence. (Sandia, 2003)

Overall, there has been resurgence in the use of red teams in the last decade, primarily because of the increased emphasis on force protection and critical infrastructure. Yet, the majority of these red teams concentrates on the technological applications of tools and weapons or assesses compliance with listed and known vulnerabilities. None truly attempt to discern new methods, applications, tools, and/or strategies of potential threat entities or attempt to evaluate the red team as a concept itself.

C. KEY ELEMENTS TO SUCCESS AND FAILURE

Although many institutions and scholars have attempted to define and describe the elements and process of models, games and simulations, very few have directed specific thought to the importance of the red team itself or as a concept. In the compilation of research for related work, the nebulous nature of the red team and its elements became apparent. Although there are various recommendations and examinations about war games and simulations, there remains no definitive guide on the use of the red team concept, especially as related to its application and effectiveness. The red team concept has evolved in the last decade into standing and temporary groups dedicated to examining assumptions and risks of an enterprise and its plans. Mostly seen in the context of computer network vulnerability assessments, these principles and elements are applicable to any system.

When applying the red team concept, it is necessary to recognize two types of critical elements that will help or hinder the red team; we have termed these situational and organizational. The situational elements are the result of either the scenario or the red-team itself: the selection of the exercise type; the initial conditions; the development of the scenario; the selection and training of the red team members; or the analysis and documentation of the results. In contrast, the organizational elements depend on the hosting enterprise: interaction with the blue team; the imposed constraints on the red team; interpretation of the results; distribution of the resulting information; and reception of the information.

1. Situational Elements

Critical to the success of any model, game, or simulation is the stated objective. There are many reasons to conduct an exercise such as education, technical or doctrinal evaluation, research, or planning. However, in order to evaluate its effectiveness or mark the team's progress, the hosting enterprise must state the purpose(s) at the outset. (Brewer & Shubik, 1979) Once the enterprise delineates the objective, it must choose the structure of the experiment, activity, or exercise, which in turn determines the type of red team required. The range of exercises varies from the truly manual free-form experiment to the automated simulation to the highly structured field exercise. Often the structure will depend on the desired purpose. For example, the automated simulation and the field exercise are more often suited for technical evaluations and procedural training, respectively. For doctrinal evaluations and strategic planning, the manual free-form experiment is more desirable.

Once the objectives and the type of exercise have been determined, the development of the scenario becomes vital.

> Little is known about the impact of a particular scenario on game play and outcomes. Even less is known about what constitutes a "good" or "bad" scenario; the scientific investigation necessary to begin to sort these matters out has yet to be undertaken, in spite of the preponderance of bad scenarios. Successful scenarios and

> scenario writers exhibit many of the characteristics of good historical accounts and good historians.(Brewer & Shubik, 1979)

Developing the scenario should take as much time as necessary, and writers should base them on historical accounts and available doctrine to the highest extent possible. The degree of realism in the scenario greatly influences the validity of the exercise.

Contributing to the reality of the scenario is the quality of the red team itself. The enterprise must staff each red team with personnel that have not only technical skills but also a vivid imagination, so that they do more than "play Red" but also "think Red". (Perla, 1990) The surrogate must experience the adversary's methods, motives, and limitations and, if possible, the operational environment. (Sandia, 2003) Moreover, temporary or rotating red team members are preferred to a permanent staff in order to bring fresh perspectives to the issue. As an experiment progresses, documentation becomes important to the evaluation of its results. "No coherent standards exist to help the gamer with documentation; the matter is left very much up to the judgment of those conducting the game." (Brewer & Shubik, 1979) The standards for documentation must be set along with the objectives in order to determine the measures of effectiveness. Again, this is dependent upon the type of experiment conducted. The automated simulations have the possibility of being quantitative and objective while the experiments designed for research and planning are more often qualitative and subjective. (Brewer & Shubik, 1979)

2. Organizational Elements

We defined the following elements to be organizational factors largely because they vary with the host enterprise. It may be obvious to handle a strategic problem with a manual exercise, but there are numerous decisions about the structure of the teams and the exercise that can affect the resulting effectiveness. (Perla, 1990) The level of interaction with a blue team is determined at the outset and is largely dependent upon the type of exercise and the objective. The quality of interaction is even more important than the required

level. The continuous progress of events in the exercise needs to reflect the actions and reactions of not only the blue team but also the red team. (Murray, 2003) If the red team's interactions are intensely scripted vice freely played, then the red team's training can be minimal. However, if any free play is required, then the quality of the interaction will depend on the training and indoctrination of the red team members into the culture of the adversary. "There is a delicate balance between creating a reasonable representation of opposing capabilities and doctrine and imposing an artificial constraint on the imagination and creativity of the players." (Perla, 1990) Realistic constraints on the red team's potential decisions and actions become crucial to the validity of the exercise results.

As previously stated, analysis and documentation is a critical situational element but the interpretation of these results can be an organizational factor. Although the major events will usually produce obvious results, often the minor details that led to the success or failure of the exercise will take time to compile into after-action reports. After compilation, the interpretation of the degree of success or the lessons learned is dependent on the host enterprise. Even quantitative results may be interpreted subjectively depending on the desires and personalities in charge of the exercise.

> Much of the decision making that gaming supports is political in more ways than one. The most pervasive 'dirty little secret' of DoD gaming is that the games often are there to support decisions and conclusions already made. (Perla, 1990)

Another aspect of interpretation is the distribution of the results to those concerned. Sometimes, the host enterprise will classify results as proprietary or dangerous in order to hide the ineffectiveness of the tested system. Furthermore, some leaders and managers will discount the information if it does not reflect their views of the system or because it exposes fallacious assumptions. (Murray, 2003) For these reasons, it is vital to establish the parameters of effectiveness prior to the conduct of the exercise. By deciding the determining factors for success early, there can be no question or

misinterpretation of the results of the exercise. In addition, the information can help other units and agencies with similar questions by establishing not only the initial distribution but also the conditions for continued distribution at the outset of the exercise or experiment.

D. MEASURES OF EFFECTIVENESS

Measures of effectiveness will always play a critical role in any organization that has to prioritize the allocation of its resources. This is even truer for exercises and experiments conducted by these organizations. As previously stated, the purpose of the red team concept is to reduce risks and increase opportunities by challenging aspects of plans, programs, and assumptions. The risks and opportunities involved are critical to the allocation of resources, the formulation of strategies, and the development of plans.

> At its most basic, the evaluation boils down to deciding whether some idea or way of looking at the problem existed after the exercise that was not generally accepted before the game was played. (Brewer & Shubik, 1979)

Although it is easier to establish these parameters for quantitative results, the often qualitative and subjective data produced by the manual and free-play games can be complex. The fact that the data is mostly non-scientific and not replicable leads many to believe that the analysis and documentation contain no tangible research results. In addition, too much unstructured documentation is inefficient to analyze or interpret. Therefore, it becomes necessary for the enterprise to identify “reasonable, interesting, and manageable units of observation and analysis.” (Brewer and Shubik, 1979) With either research or strategy as an objective, there are two potential approaches to examining the results of a manual free-play exercise: the decision-making approach and the event approach.

1. Decision-making Approach

> The manual, free-form game has great potential – though it is rarely used – as a way of examining branch points, that is, the logical development of courses considered seriously by one of the teams but not actually submitted as a formal move during gameplay. (Brewer & Shubik, 1979)

The decision-making approach attempts to examine the logic behind the selected events of the red team. The type and scope of decisions is as important as the reasons for selection. Attempting to discern the elements of the adversary's decision-making process can yield useful insights into methods of targeting, especially for information operations. However, this aspect of the adversary is the most difficult to interpret. The surrogate adversary, or red-team, truly needs to have an understanding of the enemy in order to deliver realistic insights into their decision-making process. Unlike the rational actor theory, most people do not make entirely rational decisions. Personal biases, doctrine, ideology, and experiences can sway a cost-benefit analysis to a preferred course of action.

2. Event Approach

The event approach treats each event as specific evidence for a research interest. Whether it is tactics, weapons employment, procedural ideas or branch points, these events can facilitate the exchange of information or create and challenge emerging operational concepts. Furthermore, the enterprise can formulate these events into "signatures such as data entries or intelligence reports." (Sandia, 2003) Although it is necessary to understand why the surrogate adversary chooses a specific event, the branch points can be as critical to understanding the adversarial viewpoint. Additionally, the red team can conceptualize new tactics, weapons and tools, or procedures, affording intelligence analysts and design engineers new avenues for consideration.

E. SUMMARY

The red team concept can challenge assumptions, measure risks, and increase opportunities by capitalizing on an approach that can create new knowledge or examine the decision to employ this knowledge. Yet, it requires careful application of the key situational and organizational elements in order to be effective. The selection of the exercise type, the initial conditions, the development of the scenario, the selection and training of the red team members, and the analysis and documentation of the results will largely shape the "play" of the red team. However, interaction with the blue team, the imposed constraints on the red team, interpretation of the results, distribution of the resulting information, and reception of the information can also alter any accomplishments and contributions of the red team. Yet, organizations need this type of innovative method of examining private and public systems in order to conquer today's challenges in the security environment.

> In addition to the need for appropriate analyses, several important substantive topics appear to have been overlooked by the operational gaming community – topics whose intractability to other analytic approaches is rivaled only by their importance for international affairs and national security. In our opinion, most of these topics could be investigated, at least initially, by means of free-form manual gaming techniques… Terrorism, deception, and negotiation and bargaining strategies and tactics are equally appropriate topics. (Brewer & Shubik, 1979)

Consequently, the red team concept is uniquely capable of addressing the topic of terrorism – especially the threat that it poses to domestic security issues. However, as seen in the next chapter, several aspects of terrorism pose a challenge to planners and strategists.

III. CHALLENGE OF TERRORISM

A. TERRORIST WARFARE

> Predicting future trends in terrorism has always been next to impossible. The actors involved have been few, their actions often erratic, and the behavior of small groups in society is no more predictable than that of very small particles in the physical world. (Laqueur, 2003)

However, terrorists' influence on our world is increasing. In order to adapt our strategies to counter this threat, it is necessary to attempt to understand it. It is important to remember that "[m]any terrorisms exist, and their character has changed over time and from country to country. The endeavor to find a general theory of terrorism, one overall explanation of its roots, is a futile and misguided enterprise." (Laqueur, 2003) Yet, in examining the history, principles and elements of terrorist warfare, certain trends become recognizable, trends that we can in turn influence with our actions.

1. History

In the past, groups used terrorist warfare to extract political or financial concessions from governments and other organizations. Although historians have noted incidents of terrorism as early as the Zealots-Sicarri of the first century B.C., modern terrorism began with the French Revolution, when Robespierre used tribunals to publicize the fate of the prisoners. (Cronin, 2002) In the nineteenth century, as political revolutions and reformation movements abounded throughout the globe, terrorism gained the new goal of dissolution of empires and new distribution of political power. However, this form of terrorism focused on the assassinations of heads of state and generals as symbolic targets for greater attention. The transformation of terrorism towards national self-determination began after World War I. Yet, the international character of terrorism developed after World War II, as states, such as Russia, Iran, Libya, and North Korea, covertly sponsored terrorist organizations. Terrorists began attacking targets outside their domestic region such as the 1972 Munich

Olympics massacre by the Palestinian Liberation Organization, and then these terrorist organizations began to train each other in tactics and weapons employment. During this phase, terrorists used plane hijackings, suicide bombings, and hostage taking in seemingly random attacks to gain attention for their cause and/or raise funds for their operations. By the late 1990s, there were four trends in modern terrorism: religiously motivated terrorists were more common; the number of people killed in individual attacks had increased (while the number of attacks had decreased); since 1968, terrorists targeted U.S. nationals more; and terrorists had dispersed their attacks throughout a larger region. (Cronin, 2002)

The newest phase of terrorism, often referred to as the jihad era, is the result of the continued expansion of religiously motivated terrorist organizations. Although nationalist terrorists continue to operate around the world, the growing trend is towards religious extremists attacking Western targets. Islamic terrorists operated domestically and regionally in Egypt and throughout the Middle East and North Africa since the 1920s; but as political and economic factors increased the level of Western involvement in the region, the aggression and violence turned towards the West and the symbols of its culture and economy. In 1979, Iran called for an Islamic jihad across the Middle East, inspiring and supporting other organizations in the region to use terrorism to accomplish their objectives. A loose federation of Egyptian and Arab terrorist groups from the 1970s and 1980s organized themselves and recruited others in order to fight the Soviets in Afghanistan. For these Arab Afghans, jihad was imminent; so Afghanistan and Sudan became their base of operations for training “the faithful.” (Laqueur, 2003) This organization would transform into Al Qa’ida, which began operating strategically and globally, attacking the World Trade Center in 1993, U.S. military bases in Saudi Arabia in 1995 and 1996, U.S. embassies in Kenya and Tanzania in 1998, the USS COLE in Yemen in 2000, and the Pentagon and World Trade Center in 2001. (Pape, 2003) Whatever their motivations, throughout history, terrorists have proven that they have the ability to adapt, deny, exploit and subvert mainstream culture depending on their needs. Predictions on the future

of terrorism are dire for our society, especially as technological developments and the products of globalization allow tiny sects and local groups to enact broad campaigns with minimal resources.

2. Principles

As a type of warfare, terrorism is a form of psychological operation in an asymmetric environment. Terrorists rely on surprise and deception to instill fear into their target audience and overcome the tactical advantage of their adversary.

> Surprise is even more important in terrorism than in war: there are no massive troop concentrations, no major logistic preparations, and surprise attacks can come from unexpected quarters and through unexpected tactics. Deception plays a role in terrorism planning and so does innovation. (Laqueur, 2003)

The principles of terrorist warfare shape the terrorists as they use them. The requirement to maintain the element of surprise leads to adaptability and innovation in tactics, weapons, organizational structures, and support mechanisms. Besides its open nature, urbanization and technical progress has made our society more vulnerable than before. (Laqueur, 2003) The new global terrorist organization does not depend on state sponsorship anymore but on its ability to use crime, the international monetary exchange and other assets of globalization to support its operations.

> Opponents are sensitive to the strengths as well as the weaknesses of governments; terrorists engage in a process of constant adaptation to the strategic environment. Moving to greater destructiveness may be a reaction to a need to retain the initiative as governments find means of countering existing capabilities. (Crenshaw, 2001)

In order to survive in the terrorist arena these days, the organization must know how to use the media to its advantage, how to explore modern weaponry and technology while maintaining knowledge of the conventional, how to recruit and train others, and how to maintain covert communications and operations across the globe. They “continue to exploit a tactical advantage. The militants

operate in an ever-changing constellation of cells, moving freely from country to country across the continent, guided by opportunity and fanaticism." (Golden, Butler, & Van Natta, 2004) It is the terrorists' ability to adapt that challenges us the most. While "among the infidels," Muslim terrorists modify their usual behavior, shaving their beards, consuming alcohol, or missing daily prayer - anything to avoid suspicion in alien societies. In the Madrid bombings in 2004, the "suicide bombers were replaced by triggering devices engineered with cheap cell phones." (Golden, et al., 2004) In addition, the terrorists in Madrid changed their command and control tactics by practicing communication security in the days before and after the attacks. Furthermore, "[a]s pressure on Al Qaeda's leadership mounted, the militants adapted. Radical imams took their message underground, Muslim extremists appeared to regroup into smaller, more transient cells, intelligence officials say, with fewer discernible ties to the Qaeda hierarchy." (Golden, et al., 2004) Yet, as in Western society and military, terrorist innovation is a process based on historical example, experience, and technological capability. (Crenshaw, 2001) Therefore, it is possible to imagine the potential paths in their innovative process by assessing these factors. A terrorists' "mindset, modus operandi, and target selection" based on their doctrine, public statements, and previous successful and failed plots can generate attack indicators. The endeavor to identify these indicators drives this case study, as it drives the counterterrorist agencies in their efforts to prevent future attacks and disrupt terrorist activity.

3. Current Branches in the Study of Terrorism

"The discipline of the study of terrorism is a recent development; it goes back no further than the early 1970s." (Laqueur, 2003) There are five main approaches to studying terrorism: general theory, organizations, motivations, methods, and counter-strategy. These different examinations allow for varied interpretations and understandings of the subject. General theorists attempt to examine the history of terrorism and its effect on society, while the others examine the various aspects of terrorism separately from each other. In addition,

the general theorists often attempt to track the innovations and trends in terrorism, and then debate counter-terrorism strategies. In the discussions on organization, theories about small group dynamics, hierarchical structures, secret societies, and organizational relationships have shed considerable light on the inner workings of these organizations. While observing motivations, other theorists have debated psychology versus ideology, pathology versus behavioral conditioning, and strategy versus tactic. Furthermore, the examinations of terrorist methods (suicide bombing, assassination, hijacking or kidnapping) let the scholars divine their tactics and countermeasures. "Understanding the type of terrorist group involved can provide insight into the likeliest manifestations of its violence and the most typical patterns of its development." (Cronin, 2002) Overall, the entire purpose for dissecting terrorism into these five areas is to develop policies and objectives to eradicate it from our society. Yet, for the purpose of this case study, there are mainly two relevant discussions: the role of ideology and the trends of globalization and technology.

B. ROLE OF IDEOLOGY

"An organization's success or failure is measured in terms of its ability to attain its stated political ends." (Crenshaw, 2001) As with any organization, a terrorist's doctrine provides insights into their operations. Ideological doctrine allows us to see how terrorists see the world: whom they see as their enemies, what inspires their soldiers, etc. As potential targets, we must try to analyze their doctrine in order to prevent attacks and counter propaganda.

> While it is not the only factor which determines whether a potential target is attacked; ideology provides an initial range of legitimate targets and a means by which terrorists seek to justify attacks, both to the outside world and to themselves. (Drake, 1998)

It does this by transforming people and objects into symbols, representing that with which they are fighting. Yet, other factors do remain for consideration, particularly the availability of targets and the resources of the group concerned. (Drake, 1998)

With the current trend towards religious fundamentalism in terrorism, this idea is even more relevant.

> [W]ith the attempts of Al Qa'ida under Osama bin Laden to establish something like an international coordination bureau of Muslim terrorist groups and an International Brigade, the role of Islamic terrorism became predominant and most other terrorist groups became marginal…. (Laqueur, 2003)

For this type of terrorist organization, the West, and mostly America, is the greatest threat to them. Following this, the aim of radical Islamic terrorists is to weaken the West in any way imaginable.

> In the case of al-Qaeda, much insight into its warfare proclivity can be gained by examining its training manual, which spells out missions that include destroying a nation's foreign embassies, critical infrastructure nodes (such as vital economic centers and bridges), and even places of amusement (because they are considered sinful. (Sinai, 2003)

In recent statements, Al Qa'ida leaders expanded this target set to include anyone "helping the infidels against the Muslims in any way, shape or form" even if they are good Muslims in every other manner. (MEIC, 2004) Al Qa'ida uses this ability to adapt their ideology along with their tactics to continue their attacks on Western culture. These terrorists mainly fear globalization, viewing it as the extermination of national cultures along with territorial boundaries. (Stern, 2003) This fear has even motivated the Sunni Al Qa'ida to bend their ideology in order to cooperate with the Shi'a Hezbollah terrorist group. (Stern, 2003) Yet even as they fight against globalization and Western society, these terrorists use these very same products and technology to deliver their message internationally.

C. GLOBALIZATION & TECHNOLOGY

> [T]he tools of the global information age have led to enhanced efficiency in many terrorist-related activities, including administrative tasks, coordination of operations, recruitment of potential members, communication among adherents, and attraction of sympathizers. (Cronin, 2002)

Information technology has extended the reach of terrorists, providing them access across international borders, and broadening their base for recruits and financial resources. However, globalization does not require higher technology. It requires innovation of traditional methods to cross physical and commercial borders. The Internet, mobile phones, and tools such as instant messaging allow for communication and coordination in ways not previously available. Chat rooms allow for recruitment or other tasks in covert yet public means. Al Qa'ida even attempted to recruit Latino Muslims with U.S. passports in order to recruit less suspicious looking members.(Stern, 2003) Besides the chat rooms, terrorists have used the Internet to encrypt messages, collect intelligence, publish online training manuals, and send propaganda to the media – greatly facilitating the growth and networking capacity of terrorist organizations. Al Qa'ida has proven the most adept at adopting the newest tools of technology and adapting to fit their ends.

> Over its life span, al Qaeda has constantly evolved and shown a surprising willingness to adapt its mission. This capacity for change has consistently made the group more appealing to recruits, attracted surprising new allies, and – most worrisome from a Western perspective – made it harder to detect and destroy. (Stern, 2003)

This is specifically why those concerned with defeating terrorism must radically innovate, to show a similar willingness to change not only methods of defense but also modes of thinking.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. HOMELAND SECURITY VULNERABILITY IDENTIFICATION

A. PURPOSE OF IDENTIFICATION

Since the terrorist attack on September 11, 2001, the United States has dramatically changed its response toward terrorism. Prior to that, the United States largely treated terrorist attacks as criminal acts. In that respect, the Federal Bureau of Investigation (FBI) pursued terrorists as criminals, relying on evidence gleaned from investigations. After the attack on the Pentagon and World Trade Center, "President Bush broke with that practice – and with that frame of mind – when he decided that 9/11 meant that we are at war. He decided that the U.S. would respond not with the FBI and the U.S. attorneys, but with our armed forces and every instrument of U.S. national power." (Feith, 2004) The decision to acknowledge a war with terrorists has many consequences. The major consequence was that the military became heavily engaged in combating terrorism. By involving the armed forces, the full spectrum of participation goes beyond sending combat units into Afghanistan and Iraq. The conduct of war requires strategy, tactics, intelligence, and of course, defensive measures. Strategic development, as previously seen in the Bartlett Model (Figure 1), is an iterative process that requires assessing the security environment, weighing the risks, defining national goals, formulating strategies, and planning force structures by balancing resources. (Bartlett et al, 2000) In formulating its National Strategy for Combating Terrorism, the United States decided to approach it through four main strategies: (White House, 2003)

(1) Defeat the terrorists by attacking their sanctuaries, leadership, command, control and communications, material support, and finances;

(2) Deny [terrorists'] sponsorship, support and sanctuary by ensuring other states accept their responsibility in the war on terrorism;

(3) Diminish the underlying conditions that lead to terrorism; and

(4) Defend the United States, its citizens, its domestic and foreign interests by proactively protecting and extending its defenses to ensure identification and neutralization of the threat.

To defend the United States from terrorists; the National Strategy further delineates the goal into the following objectives: (White House, 2003)

(1) implement the National Strategy for Homeland Security;

(2) attain domain awareness;

(3) enhance measures to ensure integrity, reliability, and availability of critical physical and information-based infrastructures;

(4) integrate measures to protect United States' citizens abroad; and

(5) ensure an integrated incident management capability.

In order to provide adequate defense against attacks, it becomes necessary to identify vulnerabilities and countermeasures. The national strategy does not state the preferred method for identifying vulnerabilities and developing countermeasures, allowing for an integrated approach using various methods. The responsibility belongs to everyone and each organization must continually assess itself as potential threats develop.

B. USING MILITARY OFFICERS TO IDENTIFY VULNERABILITIES

For this case study, we used military officers on red teams to focus on maritime vulnerabilities. By using military officers to identify vulnerabilities in our systems, the United States can take advantage of the officers' technical knowledge and tactical experience. By applying this knowledge to public and private systems, the military officers provide insights and avenues of attack not previously considered by the traditional security and criminal experts. In addition, the military has a professional exercise history with the knowledge base of the conduct of 'war games' and research into gaming and decision-making theory. Furthermore, the psychological indoctrination of the military is similar to that of

most terrorist groups. Yet, military officers do differ from terrorists and these differences will affect the experiment.

Through the course of their careers, military officers gain an understanding of policy, doctrine, objectives, and maneuver. Depending on the community in which they specialize, military officers are required to learn everything from small arms engagement tactics to strategic operations campaign planning. As they progress through their career, their training emphasizes national and strategic decision-making based on resource allocation, budget, threat analysis, and end-state objectives. In addition, the majority of officers regularly participate in field exercises or formal seminar games, which imparts to them the importance of the exercise elements. The military train and exercise these officers in campaign, deliberate, and crisis action planning in order to achieve strategic, operational, and tactical objectives.

Beyond their training and experience, the psychological influence of the military is extremely similar to a terrorist organization.

> Every army aims to do what the terrorist group does: to link a larger group cause with the small-group dynamics that can deliver individuals to sacrifice. Every army cuts trainees off from their previous lives so that the combat unit can become their family; their fellow-soldiers become their brothers and their fear of letting down their comrades becomes greater than their fear of dying. (McCauley, 2002)

Armies specifically nurture this psychology of sacrifice and elitism in units that focus on covert and lethal missions, such as special operations forces, very similar to terrorists' suicide bombers. By not only separating these individuals from society, but by setting them above it, certain behaviors and attitudes develop towards 'brothers' and 'others'. This discipline allows the individual to subvert himself to the collective goal, incorporating his actions into a higher strategy by making him accountable and responsible to the larger group. While individuals in other organizations may be familiar with this attitude, nowhere else is it as developed and nurtured as systematically as in terrorist organizations and military units.

Unfortunately, there are three main drawbacks to using military officers as team members. Military officers are usually generalists and not specialists. Although well educated and extremely bright, few officers fully and consistently use the technical knowledge they possess. Most units shuffle officers through different types of jobs in their early assignments in order to familiarize them with all aspects of operations. In addition, although the military extensively practices force protection, most military members are not terrorism experts. This has changed in recent years, but most officers still only have a passing knowledge garnered from the media and intelligence briefings. The other major gap in officers' background is private commerce and business. Many officers understand the principles of business and finance, but they lack experience in dealing with unions, market competitors, and local or state agencies. These factors often bring new difficulties to private enterprises that a military officer may not fully recognize. However, this unfamiliarity with the business issues may allow for an objective look at the target's security.

C. FOCUS ON MARITIME VULNERABILITIES

Another major consequence of the attack on September 11, 2001, was the intense scrutiny directed towards our transportation systems. Although aviation is critical to the U.S. economy, the maritime industry is even more vital to our way of life.

> In a 2002 simulation of a terrorist attack involving cargo containers, every seaport in the United States was shut down, resulting in a loss of $58 billion in revenue to the U.S. economy, including spoilage, loss of sales, and manufacturing slowdowns and halts in production.[1](GAO, 2003)

The six million cargo containers that pass through our ports each year represent an enormous opportunity for smuggling, as evidenced by narcotics traffic in the past. These two main factors led us to examine maritime targets: the critical nature of shipping to the economy and the security characteristics of our ports.

[1] We assume that the simulation resulted in $58 billion per day – but the source does not state the parameters.. The simulation was sponsored by Booz Allen Hamilton and The Conference Board in 2002 with representatives from government and industry. (GAO, 2003)

1. Shipping Industry

International commerce depends on seaports as critical gateways. Over 95 percent of non-North American foreign trade arrives by ship to our country, including 100 percent of certain commodities, such as foreign oil. (GAO, 2002) Approximately 90 percent of the world's cargo moves by container, with six million containers entering into the United States each year. "In 2001, approximately 5,400 ships carrying multinational crews and cargoes from around the globe made more than 60,000 U.S. port calls each year." (GAO, 2002) Due to the shift in commerce to "just-in-time" deliveries of goods, if agencies slowed the process for inspections of all or a majority of containers, the flow of goods would be "economically intolerable." (GAO, 2002) Furthermore, security measures are often too expensive for the transportation industry due to its thin profit margin. Another problem for the shipping industry is the difficulty of verifying credentials for mariners. A recent Coast Guard review of 200,000 ship operators and crewmembers identified nine possible associates of terrorist groups, almost a dozen others under warrant for arrest, and thousands of alleged cases of credential fraud. (Johnson, 2004) With the increased requirements to restrict access to sensitive areas, it is essential to identify unauthorized personnel operating with false credentials in seaports and harbors.

2. Characteristics of Ports

Seaports are often extensive in size and accessible by water and land. Located in or near major metropolitan areas, most are enmeshed within the urban infrastructure. In addition, ports combine multiple modes of transportation within one area, allowing for a concentration of passengers, high-value cargo, and hazardous materials.

> Security is made more difficult by the many stakeholders, public and private, involved in port operations. These stakeholders include local, state, and federal agencies; multiple law enforcement jurisdictions; transportation and trade companies; and factories and other businesses. (GAO, 2003)

For example, although the federal government has jurisdiction over harbors and interstate and foreign commerce, state and local governments are the main port regulators. Moreover, each port is unique in the arrangement of its management and organization.

3. Maritime Transportation Security Act

a. Background

Recognizing the difficulties inherent in securing seaports nationwide, the United States Congress passed the Maritime Transportation Security Act (MTSA) in November 2002. This act covers a broad range of programs to improve security conditions at the ports and along U.S. waterways by identifying and tracking vessels, assessing preparedness, and limiting access to sensitive areas. By combining some old agencies and creating others, MTSA addresses the various aspects of port security. The primary agency responsible is the United States Coast Guard (USCG), supported by the Customs and Border Protection (CBP) and the Transportation Security Administration (TSA). However, several difficulties continue to hinder successful implementation of the required security measures, to include funding, jurisdiction, agency reorganization, and standards. (GAO, 2003)

b. United States Coast Guard

The MTSA tasked the USCG with performing risk assessments at the nation's seaports, deploying patrols and security teams, establishing security planning and zones, and increasing ship surveillance and identification.

> Security assessments are intended to be in-depth examinations of security threats, vulnerabilities, consequences, and conditions throughout a port, including not just transportation facilities, but also factories and other installations that pose potential security risks. (GAO, 2003)

These assessments are being conducted by an independent review agency at medium-sized ports and larger, mainly due to the cost of nearly one

million dollars per report. Private stakeholders have voiced the concern that these assessments are of little utility in comparison to their own security reviews, but the USCG believes that these assessments give the comprehensive perspective necessary to validate additional security assets and personnel. In addition to the port assessments, the USCG created new rapidly deployable Maritime Safety and Security teams, designed to provide protection for strategic shipping, high-interest vessels, and critical infrastructure. As of September 2003, the USCG deployed four teams at the ports of Seattle, Galveston, Norfolk, and Los Angeles. Additional teams are budgeted in 2004 for the cities of Honolulu, San Diego, Boston, San Francisco, New Orleans, and Miami. These teams are in addition to the redeployment of the USCG cutters and vessels in accordance with its new priorities and to the establishment and review of security zones in high-interest ports.

Other USCG efforts will require long-term investment and budget allocation. One major hurdle facing the USCG is the approval of security plans for domestic and foreign vessels. According to their estimates, it will cost approximately $70 million as part of the 2004 budget and require 150 full-time personnel to review and approve individual security plans for domestic vessels and facilities. In accordance with international agreement, each country of registry must approve their vessels' security plans for force protection.[2] Yet, some flag states have suspicious records of enforcing safety requirements in previous efforts at maritime security. The USCG plans to use extensive surveillance as part of its oversight of vessels bound for U.S. waters and lacks a contingency plan in case stronger measures are necessary. The Automatic Identification System (AIS) is one of the necessary ingredients to this surveillance. Through a long-term implementation process, this system will use "a device aboard a vessel to transmit a unique identifying signal to a receiver located at the port and to other ships in the area." (GAO, 2003) Currently, only the larger domestic commercial vessels are required to install the tracking

[2]International Ship and Port Facility Security (ISPS) Code implemented on July 1, 2004 (GAO, 2003)

equipment by the end of 2004. Each set of tracking equipment costs an average of $10,000 per vessel to its owner. However, this system requires the infrastructure present in the Vessel Traffic Service system, and thus is limited to half of the nation's 25 busiest ports.[3] Expanding the coverage of the VTS will require substantial funding and investment from private and public stakeholders, to include installation and training costs estimated between $62 and $120 million. (GAO, 2003)

c. Customs and Border Protection

During the reorganization into the Department of Homeland Security (DHS), the United States created the Bureau of Customs and Border Protection (CBP) by combining the Customs Service (USCS), the Border Patrol (USBP), and elements of the Immigration and Naturalization Service (INS) and the Animal and Plant Health Inspection Service (APHIS) from the U.S. Department of Agriculture (USDA). MTSA tasked CBP with inspecting cargo and containers, to include pre-screening and establishing standards, establishing a system for identifying suspicious persons, and documenting travelers. Thus far, the CBP has established a National Container Targeting Center, refined the previous system used for narcotics, instituted a national training program for targeting personnel, and promulgated regulations to improve the quality and timeliness of data on cargo containers. In addition, their Container Security Initiative (CSI) places staff at various foreign seaports in order to coordinate directly with their counterparts in the inspection and verification of high-risk containers prior to their departure to American seaports. Another CBP effort is the Customs-Trade Partnership Against Terrorism (C-TPAT), a cooperative program between CBP and various members of the international trade community. These private companies agree to improve the internal security of their supply chains in return for the reduced likelihood that CBP will inspect their containers and cause a slowdown in their system. (CBP, 2004)

[3] Ports and regions with VTS infrastructure include Los Angeles/Long Beach, New York/New Jersey, Mississippi River, New Orleans, Houston/Galveston, Port Arthur, San Francisco, Seattle/Tacoma, Prince William Sound, and Sault Ste. Marie. (GAO, 2003)

However, the General Accounting Office (GAO) remains concerned about the progress of the CBP implementation strategy. CBP still lacks a national system for reporting and analyzing the inspection statistics, which negates any likelihood of increased success in targeting containers. In addition, data is not available by risk level, is not uniformly reported, is difficult to interpret, and is often incomplete. Although CBP has trained targeting personnel, they have yet to establish testing or certification standards. The large volume of imports and the limited resources of CBP decrease their capability to inspect all oceangoing containers without disrupting the flow of commerce. Furthermore, space limitations and safety concerns at the seaports constrain effective utilization of screening equipment. Finally, the CBP is missing the key elements of risk management in their strategy because they failed to complete a comprehensive set of criticality, vulnerability, and risk assessments to their current systems. (GAO, 2003)

d. Transportation Security Administration

In November 2001, the federal government created the Transportation Security Administration (TSA) in order to establish needed standards, to protect all transportation systems, to create a credentialing system for transportation workers, to develop security standards, to promulgate regulations to implement standards, and to monitor the execution of the regulations. Among other passenger and aviation security measures, the two main TSA initiatives that affect port security are the Maritime and Land Security Grant Program and the Transportation Worker Identification Card (TWIC). The Maritime and Land Security Grant Program provides financial assistance to help private stakeholders defray the cost of implementing security measures locally. In order to limit access to restricted areas of all transportation facilities, TSA is developing an identification card based on biometrics. Testing different technology credentialing systems on sample cards occurred in 2003. In 2004, TSA began testing the prototypes of the entire security card process, to include background checks, collecting biometric information, verifying identities, and

issuing cards. Yet, it will be a daunting task to implement the TWIC nationwide, as the agency expects to issue “five to six million identification cards a year from mid-2004 to the end of 2007.” (GAO, 2003) Furthermore, they are still consolidating input on the varied requirements, in order to develop the necessary programs and policies to implement the system across all transportation facilities.

e. Challenges implementing MTSA

MTSA faces major challenges in its implementation: the reorganization of agencies into the DHS, available funding, delineation of jurisdiction, and establishment of standards. The federal reorganization into DHS is the most extensive in over half a century and occurred five months after the enactment of MTSA. New chains of command, reporting responsibilities, and policies created more difficulties than first imagined when Congress passed MTSA. In addition, funding for implementation is scarce while costs are high. The USCG estimates that the cost of implementation of the International Maritime Organization Security code and the MTSA will be approximately $1.5 billion for the first year and $7.4 billion in the next decade. (GAO, 2003) This does not include the expenses mentioned previously for private port facility stakeholders and cargo vessel owners and operators. Prioritization for grants and other funding programs is vital to ensure that the most critical facilities are secure against attack. However, even with funding, the establishment of national standards remains a necessary requirement. Authorities need to identify a security baseline for all facilities nationwide from which they can measure vulnerability and risk. Due to the reorganization into DHS and the private/public nature of seaports, the determination of jurisdiction is essential for collaboration and coordination. With so many agencies and organizations involved, there is a high probability for a duplication of efforts, especially in intelligence and vulnerability assessments.

D. SUMMARY

Overall, the critical nature of seaports and the shipping industry coupled with the large number of potential vulnerabilities creates many opportunities for terrorists. During the initial stages of implementing the security policies, the major reorganization into DHS, the lack of funding and resources, and the technological challenges magnify the vulnerabilities. It will require extensive assessment of facilities, methods, and threats in order to secure the seaports nationwide. Although most of the concern focuses on cargo container security, there are other avenues of attack, besides smuggling devices through shipping, that could seriously hamper international trade and the U.S. economy. If we are to conduct counter-terrorist operations properly, it is essential to identify these other likely methods. The key to defensive counter-terrorism is to decrease the opportunities available to terrorists. The chance to use military officers to examine these systems allows a fresh perspective previously unavailable with criminal security experts and law enforcement officials. Countering potential terrorism requires individuals with technical and tactical knowledge, operational planning experience, and combat conditioning. The question remains: how effective will this fresh perspective be in identifying and countering potential vulnerabilities?

THIS PAGE INTENTIONALLY LEFT BLANK

V. CASE STUDY

A. INFORMAL MANUAL EXPERIMENT

Due to the prohibitive nature of the expenses associated with a national level field exercise, enterprises normally utilize a verbal scenario or seminar war game for strategic and operational level assessments. In this particular case study, five factors led to the use of an informal manual experiment:

(1) budget and time constraints,

(2) strategic nature of the campaign objective,

(3) large number of agencies involved in maritime transportation and security,

(4) lack of a sponsoring enterprise, and

(5) the adaptability and variability of terrorist organizations.

Consequently, the targeted federal and local agencies did not know that they were under scrutiny - creating certain constraints and benefits to our experiment. The first constraint on the experiment proved to make the project more realistic in its conception. The informal nature required the red teams to avoid detection and suspicion in their actions and intelligence gathering. Any required communication or meeting area would have to be publicly available as well as covert to avoid counter-intelligence. Furthermore, the manual nature of the experiment limited our use and development of ‘weapons’ and ‘tools’ to verbal descriptions. Thus, the assessment of the success of the red team depends upon the measure of the realistic nature of the verbal descriptions rather than a staged attempt of an actual attack.

B. SCENARIO

1. Constraints & Resources

The objective for the red teams was to think and act as a terrorist cell in order to plan an attack on coastal cities through maritime avenues. The

terrorists' stated doctrine and ideology dictated the sub-objectives for the attack. Each team had to decide on the target city and the actual target, the method of attack, communication and encryption methods, intelligence and research methods, meeting conditions, and an escape plan. The choice of weapons of mass destruction was not available to the team as an attack method in order to keep the experiment at the conventional level. The progression of the case study allowed each team to initially research three targets in their city, primarily using the Internet in a manner similar to Thomas' cyber planning. (Thomas, 2003) After this initial research, the teams briefed the rest of the class on their findings and then the class decided on the final targets. Once the targets were set, the teams conducted further research on the details of the target and began to plan their communications and operational methods. Additionally, each team traveled to their target city to conduct reconnaissance and surveillance. After their research trips, each team presented three possible courses of action to attack their targets. Class discussions helped each team to choose the final attack method. The final presentation contained detailed planning of the operation to include communications requirements, the team's budget, and supporting evidence to establish the realistic nature. Furthermore, each team's imaginary budget was limited to $75,000 in order to provide a more realistic nature to the exercise. In addition, following Al Qa'ida methodology, the team had to invest half of their budget as suggested by the training manual. Because so many choices were at the discretion of the team, each member's experience and background was crucial to the effectiveness of the team.

2. Team Structure & Backgrounds

Based on the style of the previous attack on September 11, 2001, the class broke into three teams in order to plan simultaneous attacks on three different cities. It was also desirous to keep the size of each cell to an operational yet functional minimum. Furthermore, in order to evaluate the differing nature on operations, the size of each team was different – creating teams of seven, five, and three members. Therefore, each team's structure was

different in their organization, background and expertise, and operational requirements. Except for one team member, all of the students were Caucasian and have a Christian religious background.[4] The students' knowledge of terrorism was limited to general knowledge gained through brief presentations and the media, so it was necessary to train them in the terrorist doctrine and provide them with direction.

[4] The one member was Asian-American, and did chose not respond to the question about religion on the Background Questionnaire.

		SEATTLE	SAN FRANCISCO	SAN DIEGO
SERVICE				
	NAVY	7	1	2
	AIR FORCE			1
	MARINE CORPS		4	
SPECIALTY				
	Surface Warfare	4	1	
	Naval Flight	2		
	Submarine	1		1
	Communications		3	1
	Infantry		1	
	Cryptology			1
UNDERGRADUATE EDUCATION				
	BA Economics	1		
	BA Speech Communications	1		
	BS Computer Science	2	1	1
	BS Political Science	1	1	1
	BS Bioenvironmental Science	1		
	BS Mechanical Engineering		1	
	BS Industrial Distribution		1	
	BA Marketing		1	
	BA Russian Studies			1

Table 1: General Composition of Red Teams

		SEATTLE	SAN FRANCISCO	SAN DIEGO
GRADUATE EDUCATION				
	MS Information Systems	7	1	1
	MS Business Administration		1	
	MS Computer Science		1	1
	MSSE Information Warfare		2	2
	MS Information Technology Management		1	
	MS Information Systems	7	1	1
RELIGIOUS BACKGROUND				
	Catholic & Roman Catholic	2	3	
	Christian	1		
	Episcopal	1		
	Protestant			2
	No Comment	3	2	1
RACE				
	Caucasian	4	2	3
	European American	1		
	No Comment	2	3	
SEX				
	Male	6	5	2
	Female	1		1

Table 2: General Composition of Red Teams (cont.)

		SEATTLE	SAN FRANCISCO	SAN DIEGO
MILITARY EDUCATION				
	Surface Warfare – Basic	3	1	
	Submarine Warfare – Basic	1		1
	Cryptology – Basic			1
	Strike Lead Attack Training	1		
	Infantry		1	
	Expeditionary Warfare		1	
	Communications & Information Systems	1	2	1
	Steam Engineering	2		
	Nuclear Power			1
	Naval Warfare College – JPME Phase 1	1		1
	Naval Science Institute			1
	Airborne Mission Commander	1		
	Combat Squad Leader		1	
	Combat Water Survival		1	
	Fire Support Coordination		1	
	Operations Security Program Manager			1
	Expeditionary Warfare – Intelligence			1
	Air Force Squadron Officer			1
	Information Systems Security Officer		1	

Table 3: Military Education of Red Teams

3. Doctrine

In order to train the officers of the class on terrorist methods and objectives, we provided the team with a previous thesis on the “Terrorist Use of Information Operations” (Buettner, Emery. & Earl, 2003), an article on “Cyber Planning as a Concept” (Thomas, 2003) and with the Al Qa’ida training manual. (”Al Qaeda Training Manual,” 2004) The previous thesis familiarized the teams with various tools and tactics of terrorists. It explained how and why terrorists attempt to influence their audiences, communicate between various cells, and facilitate their operations. Since their inception, terrorists have continuously employed what the U.S. military terms as Information Operations. With the increase in global communication, their accumulated knowledge is even more applicable to their various objectives.

From the manual, Al Qa’ida states its main mission as: “[t]he overthrow of the godless regime and their replacement with an Islamic regime.” The sub-objectives for this mission include: (”Al Qaeda Training Manual,” 2004)

1. Gathering information about the enemy, the land, the installations, and the neighbors.

2. Kidnapping enemy personnel, documents, secrets, and arms.

3. Assassinating enemy personnel as well as foreign tourists.

4. Freeing the brothers who are captured by the enemy.

5. Spreading rumors and writing statements that instigate people against the enemy.

6. Blasting and destroying the places of amusement, immorality, and sin; not a vital target.

7. Blasting and destroying the embassies and attacking vital economic centers.

8. Blasting and destroying bridges leading into and out of the cities.

Furthermore, the “military organization” is important to accomplish these missions for the following reasons: (”Al Qaeda Training Manual,” 2004)

1. Removal of those personalities that block the call's path. All types of civilian intellectuals and thinkers for the state.

2. Proper utilization of the individuals' unused capabilities.

3. Precision in performing tasks, and using collective views on completing a job from all aspects, not just one.

4. Controlling the work and not fragmenting it or deviating from it.

5. Achieving long-term goals such as the establishment of an Islamic state and short-term goals such as operations against enemy individuals and sectors.

6. Establishing the conditions for possible confrontation with the regressive regimes and their persistence.

7. Achieving discipline in secrecy and through tasks.

The other lessons from their training manual cover: recruit requirements; counterfeit currency and forged documents; military bases to include apartments and hiding places; means of communication and transportation; training; weapons purchase and delivery; and member safety (operations security).

4. Target City Selection

> Al-Qaeda's modus operandi, as demonstrated by the 11 September attacks and outlined in its training manual, involves meticulous planning, training, and precisely timed simultaneous execution. (Sinai, 2003)

We asked each team to target a separate city on the west coast of the United States based on its ability to achieve the desired objectives derived from the terrorist doctrine and ideology. Due to their economic, military, and tourist nature, the teams chose the cities of Seattle, San Diego, and San Francisco. Each of these cities is an active commercial port that supports its regional economies. In San Francisco, the landmark nature of the Golden Gate Bridge was seen as a desirous and therefore potential target. Furthermore, the naval bases in Seattle and San Diego added a significant opportunity to the teams as an avenue of attack. Once assigned with their individual cities, the next task for

the red teams was to research their respective cities in order to identify their targets and avenues of attack.

C. TARGET SELECTION

1. Seattle

Following initial research about the city of Seattle, Washington, the cell offered three targets: the Washington State Ferry system, the Space Needle, and the commercial port. Although an interesting target from the tourist perspective, the class decided the ferry offered more tourists than the Space Needle. The sheer number of tourists, commuters, and other passengers on any ferry at any one time made it a highly desirable target. Additionally, the commercial port seemed more difficult to access from land and sea, whereas the ferry terminals have to be publicly accessible by their very nature. Therefore, for the city of Seattle, the ferries stood out as the most profitable target to the teams in accordance with Al Qa'ida's secondary objective of "[b]lasting and destroying the embassies and attacking vital economic centers". ("Al Qaeda Training Manual," 2004)

2. San Francisco

For San Francisco, even though the team offered other targets such as the 3Com Park at Candlestick Point, there never could have been another target in the city as desirable as the Golden Gate Bridge. Besides being a major roadway under constant maintenance that transports thousands of motorists and pedestrians from one side of the bay to the other, the Golden Gate is a national landmark of the United States. Built during the Great Depression, it has become a symbol and testament to the American spirit. The suspension style of the bridge complicates the access through maritime tactics. However, even though San Francisco does have other potential targets that are accessible by maritime avenues, no other target would be as symbolic if successfully destroyed as the Golden Gate Bridge. Al Qa'ida further advocated this type of target in their

secondary objective of “[b]lasting and destroying bridges leading into and out of the cities.” (”Al Qaeda Training Manual,” 2004)

3. San Diego

In San Diego, due to the military presence and city layout, multiple targets are available for attack. After their initial research, the cell offered the following possible targets: Coronado – San Diego Bay Bridge, the new Petco baseball stadium of the San Diego Padres, and an in-port submarine at the base in Point Loma. Since the San Francisco cell focused on the Golden Gate Bridge, an attack on the Coronado Bay Bridge seemed redundant and superfluous. In addition, the baseball stadium is not truly accessible from maritime avenues, limiting the applicability with the theme of the experiment. Furthermore, after reviewing the objectives from the Al Qa’ida training manual, the potential attack of a naval submarine while ‘safely’ in port in the United States seemed more in line with the overall mission, specifically Al Qa’ida’s secondary objective of “[a]ssassinating enemy personnel as well as foreign tourists.” (”Al Qaeda Training Manual,” 2004)

D. COMMUNICATIONS

Communication is the most dangerous undertaking of any underground organization. The likelihood of detection increases with each message communicated outside the cell. For this reason, covert communications that are publicly available are essential to any terrorist organization. The Al Qa’ida training manual identifies their communication methods in the following manner: (1) the telephone, (2) meeting in-person, (3) messenger, (4) letters, and (5) modern devices (facsimile & wireless). (”Al Qaeda Training Manual,” 2004) Globalization and technology have only improved the accessibility to covert modes of communication. On the Internet, terrorists conduct their business and communications through electronic mail (e-mail), steganography, web logs (blogs), instant messaging, chat rooms, and public encryption. Furthermore, with anonymous surfing and e-mail capability, one can accomplish all of the above

from an anonymous IP address. With the increased availability of satellite and disposable cell phones with Internet access and text messaging, organizations can choose from more methods of communication than ever before. Of course, when it is necessary to meet in person, colleges, bars and cafes, libraries, and hotels all offer publicly accessible meeting areas that can offer privacy and seclusion to clandestine activities. The Al Qa'ida training manual even recommends secret signals and other security measures for these meetings in order to defeat potential surveillance.

Each cell leader had to decide which type of communication they would rely on during the experiment. Every member of each team had to sign up for a publicly available web-based e-mail account using a pseudonym. The Seattle team decided to use GO.com as an electronic dead-drop. The San Francisco team relied on steganography to encrypt their messages. The San Diego team used an off-line keyword encryption method with their e-mail accounts and created a blog on a publicly available website for major announcements. Furthermore, each team decided to use instant text messaging from disposable cell phones for coordination on the day of the attack.

E. RESEARCH & INTELLIGENCE GATHERING

1. Pre-deployment

Prior to their trips to their respective cities, each cell used other resources to learn as much as possible about their targets. Mainly using information obtained from the Internet, each cell found that the reconnaissance visit should either confirm or reject their tentative plans. If anyone ever wanted a piece of information, then someone has probably posted this information on the Internet. Blueprints, design plans, and system specifications were continuously available through the World Wide Web. If not directly accessible from the source's website, than other sites devoted to history, commerce, and tourism will have copies for their personnel and visitors. The teams were able to find the majority of the necessary information on the targets through the Internet including earthquake-susceptibility design studies of bridges and the precise schedule and

traffic routes of the ferry system. Libraries, experience, and textbooks provided the remaining information. After this research, each team was able to develop an initial course of action in order to focus their efforts during their surveillance trip.

2. Reconnaissance & Surveillance Trip

This focus allowed each team to spend only two days in their respective cities taking pictures and testing the boundaries of the varied security systems and plans. By actually visiting and interacting with each target, each cell found similar security problems in all three cities. Security checks, although stepped up since the September 11 attack, are still cursory in any place besides airports and military bases. Even these were lacking as team members gained access to areas that should have been off limits to anyone besides unit personnel or rent vehicles with expired identification cards and licenses. In addition, even in some areas where the team members truly had no business, they were able to use social engineering to obtain access into restricted areas without escorts.[5] In other areas, the students simply acted as if they belonged in the area, and no one ever questioned their presence. Furthermore, by acting as naïve tourists, team members were able to photograph all of these sensitive areas and potential targets, allowing the teams to examine the situations in depth after the trip.

The true benefit of the reconnaissance and surveillance trip was the familiarity with the target gained by each team member. After so much discussion and research, actually seeing and examining the target helped each team member to visualize the attack. In addition, by trying to act as covertly as possible, the team members also glimpsed the mindset of underground organizations, those that have to avoid detection and suspicion for survival. The majority of the team members stayed in different hotels and had to find their own

[5] Social Engineering is defined as “an attacker us[ing] human interaction (social skills) to obtain or compromise information about an organization or its computer systems. An attacker may seem unassuming and respectable, possibly claiming to be a new employee, repair person, or researcher and even offering credentials to support that identity. However, by asking questions, he or she may be able to piece together enough information to infiltrate an organization's network. If an attacker is not able to gather enough information from one source, he or she may contact another source within the same organization and rely on the information from the first source to add to his or her credibility.” (U.S. CERT, 2004)

meeting places to discuss their findings. Although the instructor provided us with "get out of jail" letters, the students would have considered it a matter of shame to have to use them. As previously, stated, the cells developed initial courses of action prior to the trip so each team used this trip to plan the details and test the realism and effectiveness of their attacks. Although the majority of the initial information proved viable, the cells had to reject some minor aspects of the plans after the surveillance trips. Overall, the plans would not have been as realistic and effective without the reconnaissance and surveillance trip.

F. COURSE OF ACTION DEVELOPMENT & SELECTION

After the reconnaissance visits, each cell proposed three courses of action for the attack on their respective targets. The class then met to decide which to use. The vital criterion for selection was effectiveness of the attack to the accomplishment of the overall mission. Each cell discussed the secondary effects of the attack, including potential images for media consumption and the public announcements for release after the attack. Each cell's final presentation was the detailed planning for the entire operation to include organization, communications scheme, abort/evacuation plans, transportation and lodging plan, budget allocation, deception and supporting plans and the selected course of attack with timing and supporting data. Each cell differed slightly in presentation, but each presentation relayed the potential for a highly successful attack against the selected targets.

1. Seattle

In order to disable the port of Seattle, this cell decided to attack the Washington State Ferry system that operates in the Strait of Juan de Fuca and Puget Sound. By employing five ammonium-nitrate bombs loaded on U-haul trucks onto five different ferries, the cell believed it could cause not only long-term economic damage but also immediate panic and mayhem, not to mention the death of four to six thousand tourists and passengers. The cell leader would be in the local area coordinating the attacks through cell phone and monitoring

the progress on the Internet and television. Minutes before the attack, the cell leader will contact the Mayor and local news offices by fax with a scripted message from the organization. In addition, the leader will contact the local television station and instruct them to look towards Elliott Bay for an explosive demonstration. When all the devices are successfully set on the five ferries, each operator will detonate the bomb at a pre-selected time. Although the ferry system is implementing a new security plan, the drive to satisfy consumers and meet timetables will most likely decrease the effectiveness of vehicle inspections and identification checks as security measures. Just as on September 11, 2001, the concern for family members and friends will drive residents to call the emergency phone system, virtually causing a denial of service attack, decreasing the effectiveness of emergency responders and increasing the potential for more extensive damage.

2. San Francisco

In San Francisco, the chosen course of action migrated from a maritime attack to direct action on the Golden Gate Bridge, but the plan still requires the use of a large commercial vessel as part of the deception operation. The team would pose as a construction and maintenance team in order to take direct action on one of the two main cables of the suspension system. Even if detected prior to the collapse of the bridge, the operating area is defensible and unobservable to most parts of the bridge and the Bay. Using thermite to melt through the cable, the team expects to create the illusion that the commercial vessel destroyed the bridge by crashing into one of its anchorages. Again, the cell leader will contact the media minutes before the attack and warn of the impending crash of the commercial vessel, in order to draw attention away from the cable area and to stage the news helicopters in the area for maximum media coverage. Besides the massive casualties to commuting passengers, the reconstruction and salvage efforts would dramatically influence the economy of the Bay area for months after the attack.

3. San Diego

Most of the force protection efforts around naval vessels focus on a potential small boat attack. By using a bulk cargo commercial vessel, the San Diego cell decided to annul the majority of the current security measures. The commercial vessel would drive right through the defenses and onto the submarine, fouling its hatches and partially submerging the submarine. Immediately after impact, the operators aboard the vessel would detonate the ammonium nitrate contained in the ballast tanks, in order to provide visual effects to the attack and magnify the casualties in the area. Furthermore, mixed in with the debris, the on-board operators would release some radioactive waste to spread the alarm of a “dirty bomb” and frighten the local residents and further impact the economy. The crucial element requires the commercial vessel to conduct the attack as it departs San Diego Bay, which greatly increases the danger of detection prior to the attack. This plan also incorporates a warning to the media and environmentalists and a false Emergency Broadcast calling for evacuation. Additionally, by exploding the nearby airport’s fuel farm, the cell planned to hinder the emergency responders and divert attention away from the commercial vessel as it strays from the traffic lanes. If effective, the attack would cause massive damage to the submarine and the surrounding pier area and the scare of radioactive waste would decrease tourism and commerce throughout the area.

G. SUMMARY OF VULNERABILITIES

Even though the planned attacks seem difficult and complicated, the reconnaissance visits proved to the students that a degree of success was possible, mainly due to the number and scope of vulnerabilities available for exploitation. Although each city and target had its own unique liabilities, the majority of the exploits took advantage of two major discrepancies: operations security vulnerabilities and improper security policy implementation. A few significant discrepancies did not fit in either category.

1. Operations Security Vulnerabilities

From the joint U.S. doctrine, the definition of operations security vulnerability is “a condition in which friendly actions provide operations security indicators that may be obtained and accurately evaluated by an adversary in time to provide a basis for effective adversary decision-making.” (CJCS, 1998) Although an organization may discretely plan and execute a major operation, the normal daily unit requirements may provide enough information to the adversary to give indications of our intent, movements, and preparations. Unfortunately, the old adage is true - ‘Loose lips sink ships.’ The majority of the information required for this case study did not concern military movements, but civilian state and federal organizations that previously did not have to worry about the implementation of operations security. Advertising is necessary to have a successful business and a healthy economy; however, the organizations need to screen the information that is available to the public via the Internet and media, in order to decrease the possibility of exploitation. In particular, press releases, business presentations, blueprints, and design schemes assisted the efforts of the red teams in this case study. Web cameras and other imagery allowed for standoff intelligence, surveillance, and reconnaissance. Furthermore, social engineering tactics were able to elicit even more information. Most staff were happy to discuss their work and all matters related to their operations. From security guards discussing the new procedures to construction men discussing the ways to get around them, the red teams were consistently able to find out details that provided clues to a successful attack.

2. Improper Security Policy Implementation

A security policy is only as good as its implementation. As simple as the axiom sounds, the truth of it revealed itself to the red teams during this case study. Security personnel and staff ignored the required Identification checks, baggage and vehicle searches, and loitering at the various targets. Even in areas where security personnel were vigilant at their duties, social engineering through business contacts enabled the team members to circumvent their efforts.

Businesses and tourist attractions design their security plans to minimize cost, minimize impact on customers, maintain service levels and leverage existing resources through application of a risk-based approach. Many rely on the use of surveillance equipment and detection devices to reduce the personnel required. The presence of law enforcement personnel was either ineffective or low at each site. As previously stated, team members were able to gain access to sensitive areas merely by acting as if they belonged and were never questioned by any staff or security personnel. Even other passengers and tourists ignored the team members as they took photographs and discussed the plans. After the exercise was completed, checks with these organizations and agencies such as the Federal Bureau of Investigation revealed no reports of suspicious activity matching the descriptions of the red teams had been made during the timeframe of the visits.

3. Other Discrepancies

One of the most significant discrepancies was the result of departmental reorganization. An airport fuel farm was unguarded and unobserved with open gates, allowing access for a long period without any interference. According to the red team's research, the fuel farm had belonged to the seaport, but during the shuffle into the Department of Homeland Security, the airport was supposed to take responsibility for its security. At another target, maintenance personnel leave the keys to their Cushman vehicles in the ignition and park them in a publicly accessible area. Staff personnel commonly use these vehicles throughout the site for transporting tools and personnel, acting as a passport to sensitive areas and as validation for a stranger's presence. Although the practice of leaving the keys in vehicles may have been more convenient for business and maintenance purposes, the potential risks outweigh these benefits.

Although these vulnerabilities are important to remedy, we will not measure the effectiveness of this case study merely by their identification. As discussed previously, the effectiveness of the red team can take two approaches

and we must examine all of the benefits of the case study in order to measure its success.

VI. BENEFITS OF CASE STUDY

Due to its manual seminar style, any benefits of the case study would be qualitative and subjective at best. However, its nature also allows us to consider the broader effects of the study. As previously mentioned, there are two methods to measure the effectiveness of a manual free form red team exercise: the decision-making approach and the event approach. Using the event approach, we will examine the new tools and tactics used by the red teams to emulate terrorists. The event approach will examine the innovation of the methods and means used; however, proof that these methods and means are in use by terrorists may not exist. Using the decision-making approach, we will examine new insights and assessments about terrorist organizations as highlighted by the decisions made by the red teams. The decision-making approach is much more subjective and therefore difficult to prove without a direct discussion with the adversary.

A. EVENT APPROACH

One benefit of this case study is the increase in the understanding about the terrorists' mindset and methods to the participating individuals and others. Researchers can gain an understanding by analyzing former attacks and cataloguing tactics and tools, but the red teams were able to step into the terrorists' shoes and choose the tactics and tools themselves, depending on the details of the target. In addition, the red teams proved the premise that necessity breeds innovation. Each team was able to plan a different type of attack with similar tools and tactics.

> The Madrid bombings, which killed 202 people and wounded 1700, suggested that terrorists linked to Al-Qaeda could not only modify their tactics, but also adopt a mind-set different from the one investigators thought they knew. (Golden, et al., 2004)

This adaptability is one of the most remarkable attributes of the terrorist cells linked to Al Qa'ida. The necessity to adapt to the target and avoid detection

consistently breeds new tactics and tools as seen in the plans of the red teams. Specifically, the Seattle team did not base the use of U-Haul vehicles on historical accounts of bombings but on the fact that the Washington State Ferry system moves these larger vehicles to the center of the ferry due to height limitations, ensuring that the bomb would create the maximum damage to the ferry. In San Diego, the commercial cargo vessel attacks the submarine as the cargo vessel leaves the Bay because the outbound maritime traffic lane brings the vessel closest to the submarine and provides an unobstructed angle for maneuver onto the submarine. This type of attack subverts the force protection measures around the submarine because the Navy designed these measures to counter a small-boat, similar to the USS Cole attack. However, it also thwarts the USCG standard operating procedures because their trigger for suspicious activity requires a vessel to ignore the rule that requires all vessels conducting U.S. port visits to notify the harbor authorities 48 hours prior to arrival. Additionally, the San Francisco team decided to use thermite on the suspension cable because it emits white smoke, similar to that from welding operations, as it burns through the metal and is inextinguishable by the usual means.

The red teams also identified novel concepts in their communication and coordination plans. At the time, the idea to use a web-based e-mail service as a dead drop for messages was a unique concept to the Seattle team, but in a recent issue of Al Battar (the Al Qa'ida online training magazine), the author suggests using websites as online dead drops. (Mansfield, 2004) Reports of Al Qa'ida's use of steganography suggest that the terrorists used it during the planning for the September 11 attacks. (Denning, 2004) However, it is hard to detect and decipher without the original key as the San Francisco team discovered when they used it for covert communications, especially in this age of digital imagery. In addition, the San Diego cell used a conventional off-line keyword encryption method, but the team passed the messages through an online web-based anonymous blog on baseball news. For command and control, all three teams recommended the use of text messages on disposable cell phones to signal phases of the operation. Furthermore, the Washington State

Ferry website tracks all of its vessels online through the Global Positioning System, allowing for remote command and control for the cell leader.

B. DECISION-MAKING APPROACH

Although the previous tools and tactics are important to examine, the most beneficial aspect of this case study is the hardest to document and quantify. "In particular, how and why the opponent employs his forces as he does is often the most critical element of learning and also one of the most difficult to interpret." (Perla, 1990) Intelligence collectors and analysts may be able to adapt the tools and tactics to improve indications and warning of possible attacks, but a terrorist organization greatly differs from nation states in one aspect. It relies on surprise and deception as critical elements of their operations. For a terrorist organization to be continuously successful, it must continue to adapt and change its profile to avoid detection. Therefore, it is more important to learn how and why terrorists choose their tools and tactics instead of concentrating on the tools and tactics themselves.

One observation concerns the organization of the cell itself. "The smaller the group, the more difficult it is to trace and to penetrate, the more far-fetched and strange its motivation and ideology is likely to be." (Laqueur, 2003) In addition, less communication and coordination was required for the smaller teams. In addition, these smaller teams appear less suspicious when gathering intelligence and conducting reconnaissance. The Seattle team overcame the large group disadvantage by using the online dead-drop to minimize communication requirements. In contrast, the San Francisco team transformed their cell into two smaller cells in order to decrease the detection signature. Only the leader of each smaller cell could communicate with the other cell, and the subordinate members could only communicate with their leaders.

> One of the spin-offs from successful red teaming, when it is done correctly, is to develop among those who play on red teams a deeper understanding of potential opponents and how they might think about waging a potential conflict. (Murray, 2003)

By forcing the red teams to rely on their own knowledge and experiences with few constraints, the class members were able to immerse themselves in the role of the terrorists. Although these officers will never be terrorist experts, they definitely glimpsed how a terrorist must think firsthand. Constantly concerned with detection and surveillance, each cell member must concentrate on planning the objective without compromising the overall mission.

Additionally, as we shared our results with DHS, FBI, and other city and regional agencies, the representatives came to the same conclusion: if a terrorist wants to attack a city, he can.[6] "Given the terrorist proclivity for civilian targets, for the outrageous, and for the unexpected, defense may require the protection of too many links." (Crenshaw, 2001) For the most part, those concerned with domestic security are also those responsible for the service, law, order, health, and welfare of the population they represent. Consequently, these responsibilities can color the decisions they make about security. (Murray, 2003) Additionally, one tactic or tool can capture the attention of decision-makers and blind them to other possible methods and means. For example, the emphases on the smuggling of weapons of mass destruction in a cargo container or an attack by small boat on a navy vessel are two assumptions of the DHS and DOD. These assumptions drive the decision-makers in their selection of countermeasures. The information from this case study convinced the majority of the representatives that terrorists would take advantage of any opportunity and that in order to counter terrorists, it is necessary to change perspectives. This change of perspective is the greatest benefit of the case study. Although other methods of research may offer a glimpse, the red team members truly grew to understand the advantages and limitations of being a terrorist cell planning an attack while operating covertly in an alien city.

[6] Ray Buettner, Jr., Associate Professor of Information Sciences at NPS, briefed representatives from Seattle and San Francisco agencies in preparation for a conference on Transportation Structure Vulnerabilities on June 5, 2004, on the results of this Red Team Case Study. Key officials from the City of Seattle, Port of Seattle, Washington State Department of Transportation, USCG, and City of San Francisco were present for the briefing.

VII. CONCLUSIONS

A. SUMMARY

> Red teaming will not prevent surprises. Surprise is inherent in a world dominated by chance, ambiguity, and uncertainty. But red teaming can prepare military organizations to deal with surprise. In particular, it can create the mental framework that is prepared for the unexpected and it is the skillful, intelligent adaptation to the actual conditions of war that best leads to victory. (Murray, 2003)

Although it is necessary to take precautions and research countermeasures, terrorists will find a different target or a different avenue to accomplish their objectives, so prioritization becomes critical to any type of defense. However, by identifying vulnerabilities and hardening the security around the most desirous targets, nations can hinder the efforts of terrorists and deny them the opportunity to spread their message and achieve their objective. Furthermore, by examining the tools and tactics available to terrorists, it is possible to establish intelligence profiles and threat indicators to warn of potential attacks and other operations. Red teaming can assist in all these efforts if done correctly in the right atmosphere, but it can also provide a fresh perspective to participants and recipients. Therefore, were these military red teams effective in identifying maritime vulnerabilities to terrorist attack?

The operational plans devised by the red teams in this case study definitely have the potential to further the primary objective of terrorists linked with Al Qa'ida, as stated in the available doctrine. The communication and coordination schemes are already in use by covert terrorist cells across the globe. Additionally, with so many cells worldwide, it is impossible to say that each cell uses only one method of communication. Consequently, the communication and encryption schemes utilized by the red teams are not only consistent but also representational of the potential methods in use today. In addition, terrorists have consistently used conventional explosives delivered in remarkable means. The use of commercial cargo vessels as a means of delivery would be extremely more difficult to accomplish than the plane hijackings of

September 11, 2001. However, if the captain or key crewmembers were sympathetic to the terrorists' cause, it is plausible that other crewmembers would not be aware of their plans until minutes prior to the attack. Therefore, each of the three operational plans might have achieved a high measure of success. The operations security and policy implementation vulnerabilities show the true measure of the effectiveness of the case study. It is important to establish security measures and devise countermeasures, but poor implementation and improper release of information can offset the advantages of the security measures. As a result, this case study was effective in evaluating the security environment surrounding these three coastal cities and identifying avenues of attack on these potential targets.

"But because wargames are not mere abstract diversions, the game reviewer must also comment on its accuracy or 'realism'". (Perla, 1990) Three situational elements of the red team contribute to the realism of the case study – the composition and background of the red teams, the scenario, and the conduct of play. Even though the red team members are better educated than the average terrorist, the terrorists selected to operate in foreign cultures are not the average. They are well educated in computer science, engineering, communication methods, languages, and operational planning. The critical differences lie in the nationalities and religions of the red team members vice terrorists. The visible differences in looks may account for the lack of reports of suspicious activity.[7] The military bearing of the officers may have also contributed to the success of the individuals in social engineering information from workers and staff. Yet, with the relaxed criteria for behavior of covert operatives and the online recruitment for Muslims of different heritages, it is conceivable that terrorists will no longer fit the former profile. Religious ideology is the critical element that separates the red teams from real terrorist operatives – it is especially difficult for moderate believers to appreciate the fundamentalists' conviction and their devotion to their leaders. The seminar style for the conduct

[7] There were two women on the red teams, and all of the male officers have military haircuts and no beards. Additionally, none of the red team members are of Middle Eastern descent.

of play allowed the red teams to also function as control teams (white cells) and analyze the work of the other cells. Although it may have detracted from the realism of the case study, this conduct of play allowed the red team members to discuss the potential tools and tactics at length and draw on the knowledge and expertise of the entire class as they devised their plans. However, each red team invariably drew on their own knowledge for the final plan – relying on the most familiar and established tools and tactics available and learning from previous operations. Ultimately, we believe that this aspect is also characteristic of the conduct of terrorists. Thus, although the individuals differed greatly from the terrorist profiles, the scenario and conduct of play allowed for these differences, providing a realistic effort with effective results.

As previously discussed, the benefits of a manual free form exercise are qualitative and subjective to the reviewer. "Critics have the responsibility not only to comment on whether a designer achieved his objectives, but also on whether these objectives are worth achieving." (Perla, 1990) We truly believe that the red teams achieved worthwhile objectives while allowing an examination of the concept itself. This thesis was successful in assisting the national and regional efforts in the following respects:

(1) Identification of potential vulnerabilities on desirous targets;
(2) Evaluation of possible terrorist methods and means;
(3) Examination of the decision-making process of terrorists and covert operatives;
(4) Training of the red teams and other outside agencies in the terrorist perspective and ideology;
(5) Identification of critical situational and organizational elements of the red team concept; and
(6) Establishment of two approaches to measure the effectiveness of a red team exercise.

Yet, it is important to remember that there are constraints on any war game: (Brewer & Shubik, 1979)

(1) War games are abstractions of complex realities, and require augmentation with judgment, common sense, and the usual conventional research.
(2) Consistency and relevancy depends on the skill and fortune of designers.

(3) The results depend on the skill of the players and the judgment of the controllers.
(4) Experimental testing is required to establish appropriateness, effectiveness, utility and worth.

This thesis has identified vital measures that require action to increase the effectiveness of the case study. Moreover, additional research to complement and support the efforts of this thesis will improve the utilization of the red team concept in future endeavors.

B. RECOMMENDATIONS

The key to security, domestic or otherwise, is the continuous evaluation of the security environment while mitigating the risk of the decisions made to counter threats. By using the red team concept, enterprises can draw on the perspective of the adversary to challenge their assumptions and their countermeasures. Likewise, more civilian enterprises should employ red teams to evaluate the implementation of their security plans and daily operations security. Yet, the utilization of red teams requires careful consideration. The enterprise must take into account the critical situational and organizational elements of the red team concept. Specifically, we recommend the following steps in application of the red team concept:

(1) Determine the objective(s) of the exercise, experiment, or activity at the outset, i.e. research, training, evaluation, etc.
(2) Select the type of exercise, i.e. manual or machine, field or seminar, etc.
(3) Establish the conduct of play of the exercise to include schedule, constraints, and assets
(4) Determine the level of interaction between the blue, red, and white teams (friendly, adversary, and & control groups) or constructs for field evaluations
(5) Establish means of analysis and measures of effectiveness of the exercise
(6) Establish documentation methods and means
(7) Develop the scenario, based on historical accounts and available doctrine
(8) Staff the red team with imaginative, knowledgeable personnel
(9) Train the red team in the available doctrine and ideology of the adversary
(10) Conduct exercise

(11) Interpret results of exercise based on the established measures of effectiveness
(12) Distribute the information as required
(13) Evaluate the reception of the information, i.e. actions taken, etc.

If properly employed, the red team concept can improve any system's effectiveness.

C. FUTURE RESEARCH DIRECTIONS

This thesis attempted to evaluate the effectiveness of the red team concept in the identification of maritime vulnerabilities to terrorist attack. Yet, more remains for research about the application of the concept. As the DSB recommended, a "best practices" guide is necessary to provide consistent use throughout the DOD. Particularly, standards of documentation or training for scenario development would alleviate misinterpretation of results and enhance the realism of exercises, respectively. The varied and complex usage of red teams will hinder the establishment of concrete methods, but these guidelines would assist those unfamiliar with the concept. Furthermore, more research is required to utilize the results of this thesis completely. Countermeasures, threat warning indicators, intelligence collection methods, and policy reviews are necessary to decrease these vulnerabilities to terrorist attack. Finally, civilian agencies and regional planners especially need to research the benefits of the red team concept that are available to their own organizations.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Abuza, Z. (2003) Militant Islam in Southeast Asia: Crucible of Terror. Boulder, CO: Lynne Rienner Publishers, Inc.

"Al Qaeda Training Manual," excerpts (2004). PDF version posted by the U.S. Dept. of Justice. Retrieved September 14, 2004, from http://www.usdoj.gov/ag/trainingmanual.htm

Atran, S. (2003) Genesis of Suicide Terrorism. In *Science* (Vol. 299, pp. 1534-9) Retrieved February 28, 2004, from http://www.sciencemag.org

Bartlett, H. C., Holman, P. Jr., and Somes, T.E. (2000) The Art of Strategy and Force Planning. In *Strategy and Force Planning* (3rd ed. Pt 1, Chap. 2). Newport, RI: Naval War College Press.

Brewer, G.D, and Shubik, M. (1979) The War Game: A Critique of Military Problem Solving. Cambridge, MA: Harvard University Press.

Buettner, R. Jr., Earl, R.S., Emery, N.E. (2003) "Terrorist Use of Information Operations." Monterey, CA: Naval Postgraduate School.

Burke, J. (2003) Al-Qaeda: Casting a Shadow of Terror. London: I.B. Tauris Ltd.

Byman, D. (2003) Scoring the War on Terrorism. In *The National Interest* (Summer 2003, Issue 72, pp. 75-84)

Crenshaw, M. (1988) Theories of Terrorism: Instrumental and Organizational Approaches. In Rapoport, D.C. (Ed.), Inside Terrorist Organizations. New York, NY: Columbia University Press.

Crenshaw, M. *Innovation: Decision Points in the Trajectory of Terrorism.* Conference on "Trajectories of Terrorist Violence in Europe" at the Minda de Gunzburg Center for European Studies, Harvard University, Cambridge, MA.

Crenshaw, M. (2002) *Terrorism, Security, and Power*. Presentation at the 2002 Annual Meeting of the American Political Science Association, Boston, MA.

Cronin, A. K. (2003) "Behind the Curve: Globalization and International Terrorism." *International Security*, Vol. 27, No. 3, Winter 2002/03, pp. 30-38.

Defense Science Board (DSB). Report of the DSB Task Force on "The Role and Status of DoD Red Teaming Activities," Sept. 2003. Retrieved September 14, 2004, from http://www.acq.osd.mil/dsb/reports/redteam.pdf

Della Porta, D. (1995) The Logic of Underground Organizations. In Social movements, political violence, and the state. (Chap. 5). Oxford: Cambridge University Press.

Denning, D. (2004) “Information Operations and Terrorism.” Monterey, CA: Naval Postgraduate School.

Drake, C. J. M. (1998) The Role of Ideology in Terrorists’ Target Selection. In Terrorists’ Target Selection. New York, NY: Palgrave Macmillan.

Duggan, D. P. and Hutchinson, R.L. (2004) "Red Teaming 101," Sandia National Laboratories. Retrieved February 28, 2004, from http://www.cs.nmt.edu/%7Ecs491_02/RedTeaming-4hr.pdf

Eckert, T. (2002) "U.S. 'Red Teams' Think Like Terrorists to Test Security," Copley News Service, 20 Aug. 2002. Retrieved February 28, 2004, from http://www.signonsandiego.com/news/ nation/terror/20020820-9999_1n20redteam.html

Erickson, B. (1981) Secret Societies and Social Structure. In *Social Forces* (Vol. 60, Issue 1, pp. 188-210) Retrieved February 3, 2003 from http://links.jstor.sici?sici=0037-7732%28198109%3A1%3C188%3ASSASS%3E2.0.CO%3B2-Z

Euben, R. (1995) When Worldviews Collide: Conflicting Assumptions about Human Behavior held by Rational Actor Theory and Islamic Fundamentalism. In *Political Psychology* (Vol. 16, No.1, pp. 157-178) Cambridge, MA: Blackwell.

Feith, D. J. (2004) “U.S. Strategy for the War on Terrorism,” Speech given at Political Union University of Chicago, Chicago, IL, on April 14, 2004.
Gerecht, M. R. (2002) "The Gospel According to Osama Bin Laden," *The Atlantic Monthly*, Jan. 2002. Retrieved September 14, 2004, from http://www.theatlantic.com/issues/2002/01/ gerecht.htm

Golden, T., Butler, D. and Van Natta, D. (2004) “As Europe Hunts for Terrorists, the Hunted Press Advantages,” 22 Mar. 2004, NY Times. Retrieved April 21, 2004, from http://middleeastinfo.org/article.php?sid=4096

Hanley, J. T., Jr. (1992) *On Wargaming: A Critique of Strategic Operational Gaming*, [Doctoral Dissertation, Yale University]

Hicks & Associates Inc. (2004) Web site. Retrieved September 14, 2004, from http://www.hicksandassociates.com/whatwedo/red-teaming.html

Hoffman, B. (1998) Religion and Terrorism. In Inside Terrorism. (Chap. 4) New York, NY: Columbia University Press.

House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence (2002) *Report of the Joint Inquiry into the Terrorist Attacks of September 2001* (released 2003). Retrieved September 14, 2004, from http://www.gpoaccess.gov/serialset/creports/911.html

How Terrorism Ends. (1999) U.S. Institute of Peace, Retrieved February 28, 2004, from http://www.usip.org

Johnson, K. (2004, March 5) "Probe cites possibility of terrorists on ships." USA Today, p. 3A.

Joint Publication 3-13, (9 October 1998). Joint doctrine for information operations. Washington DC: DOD Printing.

Kepel, G. (2002) Jihad: The Trail of Political Islam. Cambridge, MA: Harvard University Press.

Laqueur, W. (2003) No End to War: Terrorism in the Twenty-First Century. New York, NY: Continuum International Publishing Group Inc.

Lewis, B. (1998) "License to Kill: Usama bin Ladin's Declaration of Jihad," *Foreign Affairs*, Nov./Dec. 1998. Retrieved February 28, 2004, from http://www.foreignaffairs.org/19981101facomment1428-p10/bernard-lewis/license-to-kill-usama-bin-ladin-s-declaration-of-jihad.html

Malone, T. G., Col. (USAF) and Schaupp, R. G., Maj. (USAF) (2002), "The 'Red Team': Forging a Well-Conceived Contingency Plan," *Airpower Journal*, Summer 2002. Retrieved September 14, 2004, from http://www.airpower.maxwell.af.mil/airchronicles/apj/apj02/sum02/malone.doc

Mansfield, L. (2004) "Everything you always wanted to know about becoming a terrorist, but were afraid to ask," Northeast Intelligence Network. Retrieved April 5, 2004, from http://www.homelandsecurityus.com/albattar.htm

McCauley, C. (2002) Psychological Issues in Understanding Terrorism and the Response to Terrorism. In Stout, C. E. (Ed.) The Psychology of Terrorism. (Vol. III, chap. 1) Westport, CN: Praeger.

Merari, A. (2000) "Suicide Terrorism." Tel Aviv University.

Middle East Information Center, (n. d.) Web site. http://middleeastinfo.org/ [accessed 28 February 2004]

Miller, J. (1999) "Greetings America: My Name Is Osama Bin Laden," *Esquire*, Feb. 1999. Retrieved February 28, 2004, from http://www.esquire.com/features/articles/2001/ 010913_mfe_binladen_1.html

Murray, W. (2003) “Thoughts on Red Teaming.” Retrieved September 14, 2004, from Hicks & Associates, Inc. website: http://www.hicksandassociates.com/reports/DART-Murray-Thoughts.pdf

Pape, R. A. (2003) The Strategic Logic of Suicide Terrorism. In *American Political Science Review* (Vol. 97, N0.3, August 2003)

Parachini, J. (2003) “Putting WMD Terrorism into Perspective,” *The Washington Quarterly*, Autumn 2003.

Perla, P. P. (1990) The Art of Wargaming. Annapolis, MD: Naval Institute Press.

Rahnema, A. ed. (1994) Pioneers of Islamic Revival. London: Zed Books Ltd.

Rapoport. D. C. (2001) “Perceptions and Misperceptions of Religious Terror,” Los Angeles, CA: UCLA.

Sandia National Laboratories. (n. d.) Web site. [accessed 14 September 2004]

Sandoz, J. F., "Red Teaming: A Means to Military Transformation," Institute for Defense Analyses, Joint Advanced Warfighting Program. Retrieved September 14, 2004, from http://stinet.dtic.mil/cgi-bin/fulcrum_main.pl?database=ft_u2&searchid=0&keyfieldvalue=ADA388176&filename=%2Ffulcrum%2Fdata%2FTR_fulltext%2Fdoc%2FADA388176.pdf

Sinai, J. (2003) "How to Forecast and Preempt al-Qaeda’s Catastrophic Terrorist Warfare," *Journal of Homeland Security*, Aug. 2003. Retrieved on September 14, 2004, from http://www.homelanddefense.org/journal/Articles/displayarticle.asp?article=37

Sinai, J. (2003) "Red Teaming the Terrorist Threat to Preempt the Next Waves of Catastrophic Terrorism," briefing delivered at the 14th annual NDIA SO/LIC Symposium and Exhibition, Feb. 2003. Retrieved on September 14, 2004, from the Red Team Journal website: http://www.redteamjournal.com/resources/sinai.pdf

Stern, J. (2003) The Protean Enemy. In *Foreign Affairs* (July/August 2003) Retrieved April 21, 2004, from http://foreignaffairs.org/20030701faessay15403/jessica-stern/the-protean-enemy.html

Sun Tzu. (1963) The Art of War. New York, NY: Oxford University Press.

The Al-Battar Training Camp. (2004, January 6). *Middle East Information Center,* No. 637. Retrieved February 28, 2004, from http://middleeastinfo.org/article.php?sid=3820

Thomas, T. (2003) Cyber planning as a concept. Parameters. Spring 2003. Retrieved February 26, 2003 from the World Wide Web.

Terrorism Research Center. (n. d.) Web site. http://www.terrorism.com/ [accessed 14 September 2004)

Tucker, J. B. (2000) Lessons from Case Studies. In Tucker, J. B. (Ed.), Toxic Terror: Assessing Terrorist Use of Chemical and Biological Weapons. Cambridge, MA: MIT Press.

U.S. Computer Emergency Response Team. (n. d.) Web site. http://www.us-cert.gov/cas/tips/ST04-014.html [accessed 14 September 2004]

U. S. Customs and Border Protection Bureau. (2004) Web site. http://www.cbp.gov/xp/cgov/home.xml [accessed 14 September 2004]

U.S. General Accounting Office. (05 August 2002) *Port Security: Nation Faces Formidable Challenges in Making New Initiatives Successful*. (Publication No. GAO-02-993T) Retrieved September 14, 2004, from GAO Website: http://www.gao.gov/new.items/d02993t.pdf

U.S. General Accounting Office. (12 December 2003) *Posthearing Questions Related to Aviation and Port Security.* (Publication No. GAO-04-315R) Retrieved September 14, 2004, from GAO Website: http://www.gao.gov/new.items/d04315r.pdf

U.S. General Accounting Office. (09 September 2003) *Maritime Security: Progress Made in Implementing Maritime Transportation Security Act, but Concerns Remain* (Publication No. GAO-03-1155T). Retrieved September 14, 2004, from GAO Website: http://www.gao.gov/new.items/d031155t.pdf

U.S. General Accounting Office (16 December 2003) *Homeland Security: Preliminary Observations on Efforts to Target Security Inspections of Cargo Containers* (Publication No. GAO-04-325T) Retrieved September 14, 2004, from http://www.gao.gov/highlights/d04325thigh.pdf

White House. (2003) National Strategy for Combating Terrorism. Washington DC: White House, February 2003.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

Defense Technical Information Center
Ft. Belvoir, Virginia

Dudley Knox Library
Naval Postgraduate School
Monterey, California

Raymond Buettner, Jr.
GSOIS, Naval Postgraduate School
Monterey, California

Dorothy Denning
Naval Postgraduate School
Monterey, California